NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEPLOYMENT OF 802.15.4 SENSOR NETWORKS FOR C4ISR OPERATIONS

by

Damian N. Ngo

June 2006

Thesis Advisor:	Gurminder Singh
Second Reader:	Rex Buddenberg

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE: Deployment of 802.15.4 Sensor Networks for C4ISR Operations	5. FUNDING NUMBERS
6. AUTHOR(S) Damian N. Ngo	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The applications of wireless sensor networks (WSNs) have risen in recent years both in the civilian and military sectors. While a number of WSN-based systems have been proposed and developed, vast majority of them focus on capability demonstration rather than the issues of deployment. As a result, even though the systems can serve useful purposes, they are very hard to deploy. The objective of this thesis is to focus on the deployment issues of WSNs. In addition, this thesis assesses the optimal configurations and environment that enables the sensor networks to thrive in a C4ISR environment.

This thesis presents a technology review of the ZigBee and the IEEE 802.15.4 standards which form the core technology in WSNs. The thesis also discusses the IEEE 802.15.4 Physical and Media Access Control Layers that comprise the bottom two layers of WSNs.

This thesis also provides a brief introduction to the hardware and software that deal with WSN technology.

Lastly, this thesis evaluates the military applications of WSNs. It is hoped that the military can employ wireless sensors to increase situational awareness, attain information superiority, and improve decision-making.

14. SUBJECT TERMS Wireless sensor networks, ZigBee, deployment issues, Crossbow motes, sensor nodes	15. NUMBER OF PAGES 95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEPLOYMENT OF 802.15.4 SENSOR NETWORKS FOR C4ISR OPERATIONS

Damian N. Ngo
Lieutenant, United States Navy
B.S., Hampden-Sydney College, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2006

Author: Damian N. Ngo

Approved by: Gurminder Singh
Thesis Advisor

Rex Buddenberg
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The applications of wireless sensor networks (WSNs) have risen in recent years both in the civilian and military sectors. While a number of WSN-based systems have been proposed and developed, vast majority of them focus on capability demonstration rather than the issues of deployment. As a result, even though the systems can serve useful purposes, they are very hard to deploy. The objective of this thesis is to focus on the deployment issues of WSNs. In addition, this thesis assesses the optimal configurations and environment that enables the sensor networks to thrive in a C4ISR environment.

This thesis presents a technology review of the ZigBee and the IEEE 802.15.4 standards which form the core technology in WSNs. The thesis also discusses the IEEE 802.15.4 Physical and Media Access Control Layers that comprise the bottom two layers of WSNs.

This thesis also provides a brief introduction to the hardware and software that deal with WSN technology.

Lastly, this thesis evaluates the military applications of WSNs. It is hoped that the military can employ wireless sensors to increase situational awareness, attain information superiority, and improve decision-making.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

BS	Base Station
CCA	Clear Channel Assessment
CID	Cluster Identifier
CLH	Cluster Head
COASTS	Coalition Operating Area Surveillance and Targeting System
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
FFD	Full-Function Device
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
IT	Information Technology
LAN	Local Area Networks
LOB	Line of Bearing
LQI	Link Quality Indication
MAC	Media Access Control
MAN	Metropolitan Area Networks
MEMS	Micro Electro-Mechanical Systems
MSP	Mote Security Package
NLOS	Non Line of Sight
OSI	Open System Interconnection
PAN	Personal Area Networks
PHY	Physical
PIR	Passive Infrared
PSK	Phase Shift Keying

RF	Radio Frequency
RFD	Reduced-Function Device
SRAM	Static Random Access Memory
TCP/IP	Transmission Control Protocol/Internet Protocol
TinyOS	Tiny Micro Threading Operating System
UARTs	Universal Asynchronous Receive and Transmit
UAVs	Unmanned Aerial Vehicles
WAN	Wide Area Networks
WLAN	Wireless Local Area Networks
WPAN	Wireless Personal Area Networks
WSNs	Wireless Sensor Networks

ACKNOWLEDGMENTS

This thesis is dedicated to my lovely wife who has always been supportive of my naval career. Her love, encouragement, and support have guided me along throughout our years together.

I would also like to acknowledge my advisors, Gurminder Singh and Rex Buddenberg, for their guidance and support throughout my thesis process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The “Information Age” has affected every aspect of our lives. Technology has led to many innovations that have expanded our boundaries and shrunken the dimensions of time and space. One new technology that is attracting significant attention is wireless sensor networks (WSNs). WSNs have generated a lot of interest from both the military and civilian sectors because of their capability to collect and process data from remote locations (Brownfield, 2005). There are many applications of WSNs. For example, WSN can be deployed in a factory warehouse to sense and monitor environmental conditions. For the military, WSN can be deployed to conduct surveillance missions by detecting moving objects such as a tank or car. All these applications of WSN make them very attractive and have propelled the research of wireless sensors.

Wireless sensor networks consist of sensors and wireless networking. The sensors are devices capable of sensing their environment, computing data that have been collected, and disseminating that data to a designated base station. The sensors operate in a wireless networking environment that is self-healing and self-organizing. One type of wireless technology is ZigBee. ZigBee is a new industrial standard for ad hoc networks based on IEEE 802.15.4 (Ding, 2005). The 802.15.4 standard covers the Medium Access Control and the Physical Layer of networking while ZigBee extends 802.15.4 to cover the networking and application side. ZigBee technology emphasizes on low cost battery powered applications. In addition, ZigBee is best

suited for low data rate, short range communications. This technology is not intended to replace 802.11, Bluetooth, or any other standards. Instead, ZigBee capitalizes on its capabilities and provides applications to the consumers that are reliable and cost effective. As the business world finds new ways to implement ZigBee technology, more ZigBee enabled products are being developed. Wireless sensor networks and ZigBee technology are not a trend that will quickly fade. They are valid technology that will impact our lives and culture.

B. OBJECTIVES

The IEEE 802.15.4 and ZigBee standards have come into existence in the last 2-3 years only. Though recently developed, they have shown great promise in remote sensor applications. The applications of this technology are viable for both the military and commercial world. The objective of this thesis is to focus on the deployment issues of WSNs. In addition, this thesis intends to assess the optimal configurations and environment that will enable the WSNs to thrive in a C4ISR environment.

C. RESEARCH QUESTIONS

The primary target of this thesis is the deployment issues of WSN systems. The study addresses the following questions.

- What is a sensor network?
- What are the characteristics of WSN?
- What are the standards of 802.15.4?
- What is ZigBee?
- What are the characteristics of ZigBee?
- What are the applications of ZigBee?
- What are the vulnerabilities of ZigBee?

• What are the existing hardware and software that incorporate ZigBee technology?
• What are motes?
• How are motes deployed in a sensor network?
• How are nodes distributed to maintain effective network connection?
• How many nodes are required to maintain effective network connection?
• What is the optimal range between nodes?
• What is the duration of battery life used in Crossbow motes?

D. SCOPE

The scope of this thesis covers an overview of wireless sensor networks, with an emphasis on ZigBee wireless technology. Thus, the research is divided into two parts. The first part focuses on WSN and their characteristics. The focus then narrows down to evaluating the Crossbow WSN products. The second part of the research deals with the implementation and testing of a WSN system developed at NPS. The testing focuses on the hardware and software that are provided by Crossbow, in particular the MSP410CA Mote Security System.

E. METHODOLOGY

This thesis uses the following methodology to fulfill its requirements:
• A comprehensive review of scientific literature on WSN.
• Analysis of the IEEE 802.15.4 standards.
• Analysis of wireless sensor experiments using the Crossbow MSP410CA Mote Security System.

F. THESIS ORGANIZATION

This thesis is organized as follows. Chapter II provides an overview of wireless sensor networks with an introduction to the sensor nodes, development of WSN, and the WSN architecture. The chapter also provides an overview of WSN applications, constraints, and challenges. The second half of Chapter II deals with the history of the ZigBee working group and the adoption of the IEEE 802.15.4 standard. In addition, ZigBee 802.15.4 wireless technology is also discussed to include an overview of the 802.15.4 standards, Physical layer, and MAC layer. The chapter concludes with the discussion on ZigBee networks topologies.

Chapter III discusses the military applications of WSNs. The chapter begins with the objectives and criteria that the military wants to address concerning WSNs. It provides strengths and weaknesses of WSNs that the military can face when they implement this technology. The chapter concludes with examples of wireless sensors that are available and the applications of these sensors by the military.

Chapter IV is an overview of the Crossbow MSP410CA Mote Security System that is used in this thesis research. In addition to the surveillance system, a brief discussion on other Crossbow hardware and software products is provided.

Chapter V begins with a discussion on the Crossbow MSP410CA Security System used by the Coalition Operating Area Surveillance and Targeting System (COASTS) at the Naval Postgraduate School. The chapter also covers the implementation and testing of the Crossbow security system that is used in this research. Observations from the test

results are also provided. The chapter concludes with deployment issues that a user may face when implementing a WSN similar to the Crossbow security system.

Chapter VI includes an overview of the entire research and makes recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS SENSOR NETWORKS

A. INTRODUCTION

The focuses of this chapter are to describe wireless sensor networks (WSNs) and the 802.15.4 ZigBee technology. It provides a brief overview of WSN in terms of their characteristics, capabilities, applications, and limitations. The chapter begins with a description of sensor nodes which are the building blocks of the WSN. From the sensor nodes, the chapter moves on to WSNs. After the discussion of WSNs, the chapter moves on to ZigBee technology. A brief history of ZigBee and the working groups is discussed. In addition, ZigBee standards, the Media Access Control (MAC) layer, the physical layer, and network topologies are discussed in this chapter.

B. SENSOR NODES

The advancement of technology in recent years has fostered new innovations and technical capabilities. Computer processing speed has increased exponentially while the size of the chip has dramatically decreased. These technical advances have shown that Moore's law is very much valid in the information technology industry.

1. The Rise of the MEMS

Technical advances over the years have made it possible for researchers to develop large variety of Micro Electro-Mechanical Systems (MEMS). MEMS are "miniaturized low-power devices that integrate sensing, special purpose computing and wireless communications capabilities" (Wadaa, 2005). These small devices are also known as sensor nodes.

Sensor nodes are MEMS devices that possess three basic capabilities. These capabilities include sensory,

computation, and wireless communication. Figure 1 illustrates the capabilities of the sensor nodes and demonstrates the basic components of these nodes. The components include sensing, data processing (CPU), and communicating.

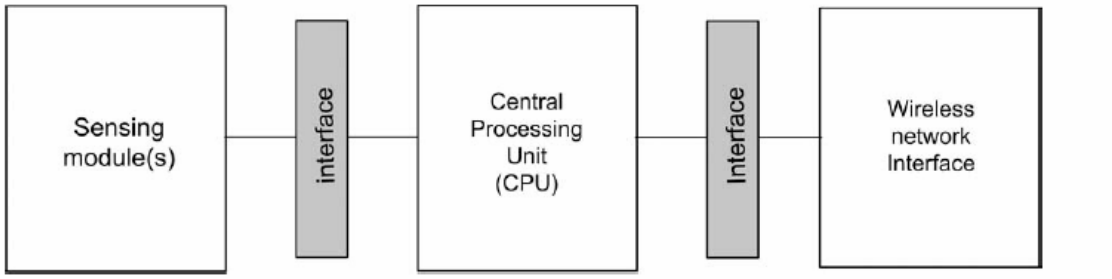

Figure 1. Breakdown of a sensor node (Wadaa, 2005).

2. Sensor Nodes Capabilities and Constraints

The sensory component found on sensor nodes is used to acquire data from their environment. Depending on the sensor nodes, some nodes are able to sense temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence of absence of certain kinds of objects, mechanical stress levels on attached objects, and the current characteristics of an object of interest such as speed, direction, and size of the object (Piorkowski, 2005). The computational capability is needed for aggregating data, processing control information, and managing both sensory and communication activity. The wireless communication capability is used for sending and receiving aggregated data and control information to and from other sensors (Wadaa, 2005).

In addition to their capabilities, sensor nodes also have constraints that need to be mentioned. These constraints include:

a) Sensor nodes are often anonymous

b) Sensor nodes are small

c) Sensor nodes often have a non-renewable energy supply

d) Sensor nodes have a modest transmission range

e) Sensor nodes are usually deployed unattended

Sensor nodes are invaluable devices whose applications in the military and civilian sector are expanding each day. However, in order to effectively apply sensor nodes, both capabilities and constraints must be understood.

3. Hierarchy of Sensor Nodes

Though sensor nodes are small simple devices, there are many types of nodes with different functions. To help understand the different types of nodes, a hierarchy view is used to describe the nodes. The hierarchy for sensor nodes has four levels. The bottom level consists of low level sensors while the top of the hierarchy contains sensors capable of high level data aggregation, analysis, and storage. Each tier has different level of sensors capable of different types of sensing. The four tiers of the hierarchy are illustrated in Figure 2.

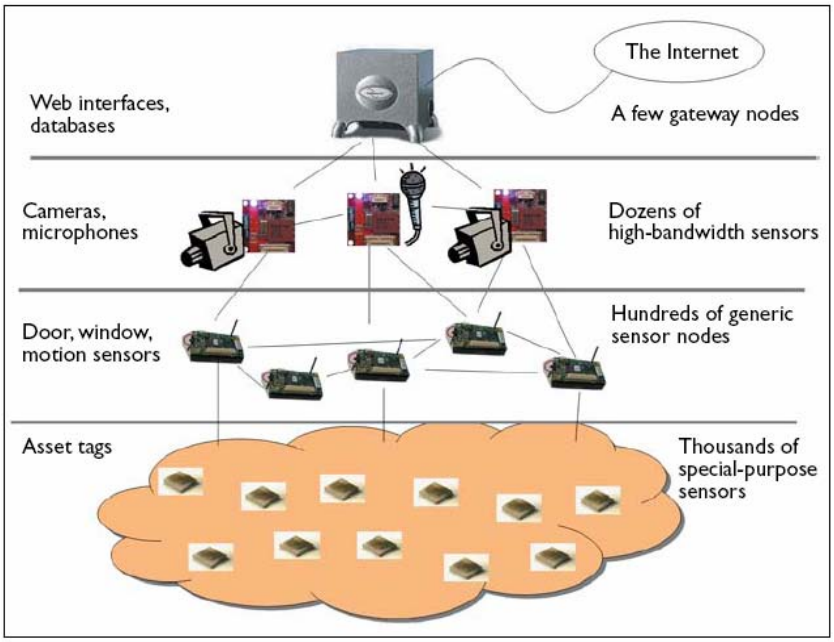

Figure 2. Hierarchy of sensor nodes (Hill, 2004).

a. Special Purpose Sensor Nodes

The bottom tier of the hierarchy contains simple, special-purpose sensor nodes, also known as "smart dust," designed to track assets of interest. These tiny devices are powered by limited energy sources (such as batteries) and are triggered when an asset moves in or out of a protective zone. These devices can be attached to merchandises in a warehouse and serve as an anti-theft device. If an intruder enters the warehouse and takes some merchandise with a smart dust attached, an alarm is triggered which alerts warehouse security of the intrusion.

b. Generic Sensor Nodes

The second tier in the hierarchy consists of generic sensor nodes which have higher capability than the smart dust. On a similar theme about warehouse security, these nodes can be placed by windows and doors to detect unauthorized access into the warehouse. Once an intruder

is detected, the sensor node transmits its data to a sink node or base station. The sink node serves as a data repository for the other sensor nodes that do the data sensing and collecting.

An example of a generic sensor node that is available today is the Mica2 Mote. The term “mote” refers to a general class of technology that aims to produce small, robust, and versatile sensors that can be easily deployed over a wide area (Icus, 2006). The Mica2 mote is a third generation mote module developed by Crossbow Corporation for the purpose of enabling low-power wireless sensor networks (Crossbow, 2005). Figure 3 illustrates a Mica2 mote.

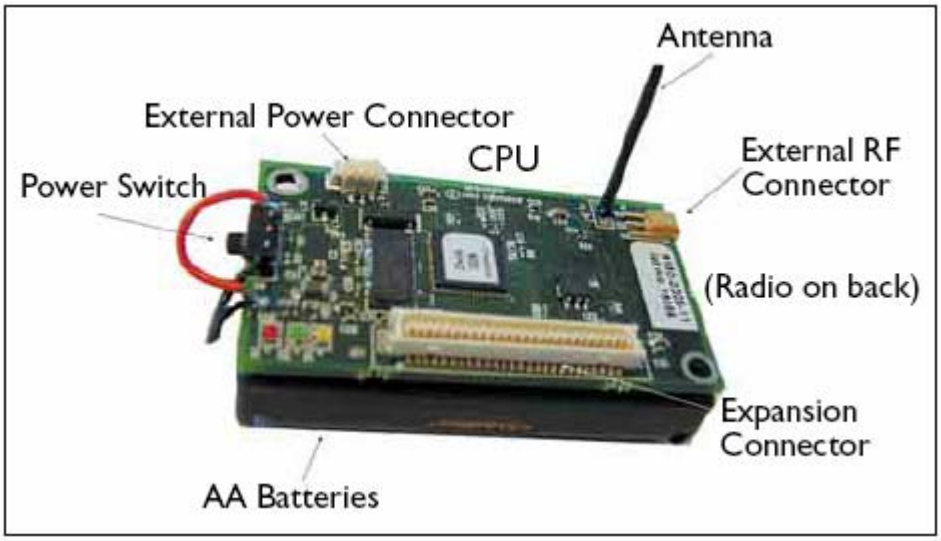

Figure 3. Mica2 Mote (Hill, 2004).

c. High-Bandwidth Sensor Nodes

Moving from simple nodes to high level data aggregation, the third tier sensor nodes have higher computational and communication capabilities. These nodes are referred to as high-bandwidth sensors and are used to

transmit video or audio signals. Unlike the first two classes of nodes, the high-bandwidth sensors require greater power. In some instances, the nodes are plugged into an electrical outlet.

d. Gateway Nodes

The last type of nodes is called gateway nodes. They are designed to process and store sensor reading from the other nodes. The gateway nodes serve as an interface into other existing networks. The hierarchy is complete containing gateway nodes at the top serving as a central station with databases and aggregation software. Table 1 provides a breakdown of the four nodes and their basic operational characteristics.

Node Type	Sample "Name" and Size	Typical Application Sensors	Radio Bandwidth (Kbps)	MIPS Flash RAM	Typical Active Energy (mW)	Typical Sleep Energy (uW)	Typical Duty Cycle (%)
Specialized sensing platform	Spec mm^3	Specialized low-bandwidth sensor or advanced RF tag	<50Kbps	<5 <0.1Mb <4Kb	1.8V*10–15mA	1.8V*1uA	0.1–0.5%
Generic sensing platform	Mote 1-10cm^3	General-purpose sensing and communications relay	<100Kbps	<10 <0.5Mb <10Kb	3V*10–15mA	3V*10uA	1–2%
High-bandwidth sensing	Imote 1-10cm^3	High-bandwidth sensing (video, acoustic, and vibration)	~500Kbps	<50 <10Mb <128Kb	3V*60mA	3V*100uA	5–10%
Gateway	Stargate >10cm^3	High-bandwidth sensing and communications aggregation Gateway node	>500Kbs–10 Mbps	<100 <32Mb <512Kb	3V*200mA	3V*10mA	>50%

Table 1. Operating characteristics of the four different sensor nodes (Hill, 2004).

C. OVERVIEW OF WIRELESS SENSOR NETWORKS

The arrangement of sensor nodes around an area of interest for the purpose of forming a sensing, data collection, and communication infrastructure forms a wireless sensor network. The advancement of information technology over recent years has enabled wireless communications to evolve toward a point where WSNs are economically feasible and operationally effective. WSNs are characterized as being dynamic and autonomous networks capable of self organizing and self healing. In addition, they are also highly flexible with the capability for rapid deployment. Coupled with these qualities and the low cost of WSNs, the applications of WSNs are bound to significantly increase in the near future.

D. WIRELESS SENSOR NETWORKS CHARACTERISTICS

Based on the sensor nodes that are deployed, there are two categories of WSNs. The first category of WSNs is called a homogeneous sensor network. Homogeneous WSNs consists of identical nodes, sharing the same sensing, computing, and communication capabilities. The second category of WSNs is the heterogeneous wireless sensor network consisting of sensor nodes with different capabilities.

1. Deployment of Sensor Nodes

The deployment of sensor nodes in a WSN can be accomplished using two types of methods. The first method deploys nodes in a random fashion. The nodes are scattered over an area via helicopter or low flying plane. Due to the autonomous nature of the nodes, operators are not required to continuously man the sensory devices. The second method distributes the nodes in fixed locations. The sensing nodes and the sink node are carefully placed by

operators in locations that are considered areas of interest. Figure 4 is an illustration of a deployment of WSN where the circles represent sensor nodes and the black square is a sink node.

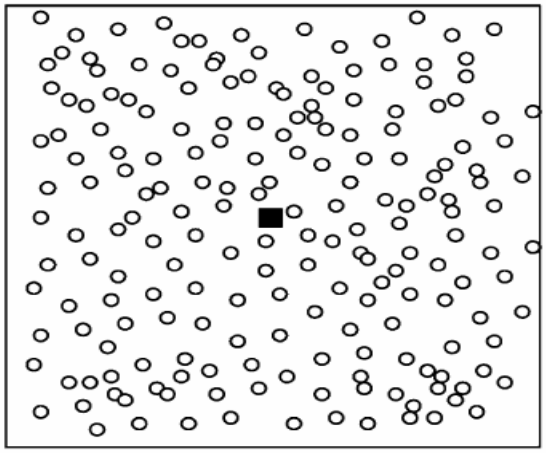

Figure 4. A sensor network (Wadaa, 2005).

The nodes that make up the WSN are comprised of four components:

a) sensors

b) wireless communications

c) data processing

d) power supply (i.e., battery)

In addition, the sensory nodes can be in four different modes during their operation:

a) transmitting a message

b) receiving a message

c) sensing an event (e.g., light, pressure, temperature)

d) sleeping

The sleep mode is used to describe a sensory device that is not communicating with other devices and is not sensing an event.

E. WIRELESS SENSOR NETWORKS APPLICATIONS

WSN have become a viable solution for sensing and collecting data in a number of applications. The civilian and military sectors can find valuable applications in WSNs. Some of these applications are listed below.

Environmental applications:

- Forest fire detection
- Biocomplexity mapping of the environment
- Flood detection
- Precision agriculture

Health applications:

- Telemonitoring of human physiological data
- Tracking and monitoring patients and doctors
- Drug administration

Home applications:

- Home automation
- Home security
- Smart environment

Commercial applications:

- Environmental control in office building
- Managing inventory control
- Vehicle tracking and detection

Military applications:

- Troops identification
- Securing buildings or perimeter
- Monitoring battle space
- Enemy detection (Rajaravivarma, 2003)

The list of WSN applications that is provided above is only a partial list. With time, the use of WSN will become pervasive in many more aspects of our lives.

F. WIRELESS SENSOR NETWORKS CHALLENGES AND CONSTRAINTS

Wireless sensor networks can be valuable assets. However, in order to best utilize these assets, their challenges and constraints must be understood. One of these challenges is the power limitation of the sensor nodes. Unlike cell phones and PDA's, WSN don't have the capability for periodic recharging. WSN are designed to be deployed in the field without maintenance or human intervention. The lack of human intervention means that the nodes can only operate as long as the lifetime of the battery. Another challenge is that WSN are limited in power, computational capabilities, and memory. These capabilities are limited so that the sensor nodes can be small and inexpensive. In addition, since the sensor nodes are small and inexpensive there is a high risk of the nodes failing during their deployment. As a result of the nodes failing, the WSN topology may have to change rapidly. To overcome the failing nodes and changing topology, it is necessary to have large scale networks consisting of thousands of sensor nodes which provide sufficient redundancy.

G. WIRELESS PERSONAL AREA NETWORKS

There are many types of wireless networks. These networks are categorized based on the geographic scale of their coverage. Going from largest coverage to smallest, the Wide Area Networks (WAN) are first, followed by the Metropolitan Area Networks (MAN) which cover a city area. The Local Area Networks (LAN) are smaller than the MAN and cover a campus size area. The smallest networks are the Personal Area Networks (PAN) and their coverage is limited

to the size of a room. The wireless PAN are the focus of this chapter and they are implemented in ZigBee wireless devices.

H. 802.15.4 HISTORY AND THE WORKING GROUPS

There are many applications of wireless sensor networks in the industrial, military, and home markets. Before the introduction of ZigBee wireless technology into the market, sensors and control devices that were in the market used high bandwidth and high data rates. The technological standards prior to ZigBee meant that sensor devices were complex, costly, and required a large amount of power. These standards did not meet the needs of researchers and designers who wanted wireless sensors to be smaller, be less complex, consume lower amount of energy, and require lower data rates. These wireless needs pushed researchers toward ZigBee technology that promised to provide reliable, secure, low power, and low cost networks.

1. History of the ZigBee Alliance

ZigBee wireless network technology was initially developed in 1999 by the Firefly Working Group (Geer, 2005). Over time, the Firefly Working Group faded away and the ZigBee Alliance emerged as the driving force to push the standards for a secure, reliable, low data rate, and low power consumption wireless network. The ZigBee Alliance is composed of over 175 industry leaders from 29 countries (ZigBee.org, 2006). These industry leaders come from companies that include chip suppliers, wireless IP providers, OEMs, and test equipment manufacturers. The alliance has eight promoting companies that include Chipcon, Ember, Freescale, Honeywell, Mitsubishi, Motorola, Philips, and Samsung. The ZigBee Alliance is a strong entity with the mission to define “a complete open global

standard for reliable, cost-effective, low power, wirelessly networked products addressing monitoring and control" (ZigBee.org, 2006). With this mission in mind, the alliance set out to provide the markets with three services. These services include products branding, compliance and certification testing, and defining the application profiles (Craig, 2005).

2. The IEEE 802.15.4 Working Group

The ZigBee Alliance wanted wireless applications that would meet the needs of its low data rate, low complexity, and low cost network sensors. Fortunately, the wireless applications that the alliance sought had a standard that was developed by the IEEE 802.15 working group.

The IEEE 802.15 is the 15th working group of the IEEE 802 which focuses on wireless personal area network (WPAN). The 802.15 has four task groups. Task group one deals with the Bluetooth 1.0 standard. Task group two focuses on the coexistence of WLAN and WPAN. Task group three is responsible for developing high rate WPAN standards. Lastly, task group four specializes in devices that use low rate WPAN but have long battery life.

3. ZigBee 802.15.4 Technology

The ZigBee Alliance adopted IEEE 802.15.4 as the media access control (MAC) and physical (PHY) layer standard in 2003 (Ding, 2005). Soon after that, the alliance ratified the first ZigBee standard for network and higher layers in December 2004. These standards ratified by the ZigBee Alliance were released to the public in June 2005 (Geer, 2005).

Figure 5 below is an illustration of the areas of responsibilities among the IEEE standard, ZigBee Alliance, and the users. In the figure, it shows that the IEEE

802.15.4 standard specifies the PHY and MAC layers. The PHY and MAC layers will be discussed in details later in the chapter. The figure also shows that the ZigBee Alliance specifies the standards for the network layer and the application layer. Lastly, the application profiles are also defined by the ZigBee Alliance.

The addition of ZigBee to the IEEE 802.15.4 standard has been an improvement to wireless network technology. Although IEEE 802.15.4 supports mesh and other network technologies, its standard only operates peer to peer. However, with the addition of ZigBee network layer greater capabilities are achieved in wireless technology. This implies that the ZigBee network layer allows the 802.15.4 technology to work with other network topologies (Ding, 2005). Instead of being limited by peer to peer connection, ZigBee technology can multi-hop so that any two sensor nodes can communicate with each other by utilizing neighboring nodes. In addition, ZigBee technology provides security to the IEEE 802.15.4 standard.

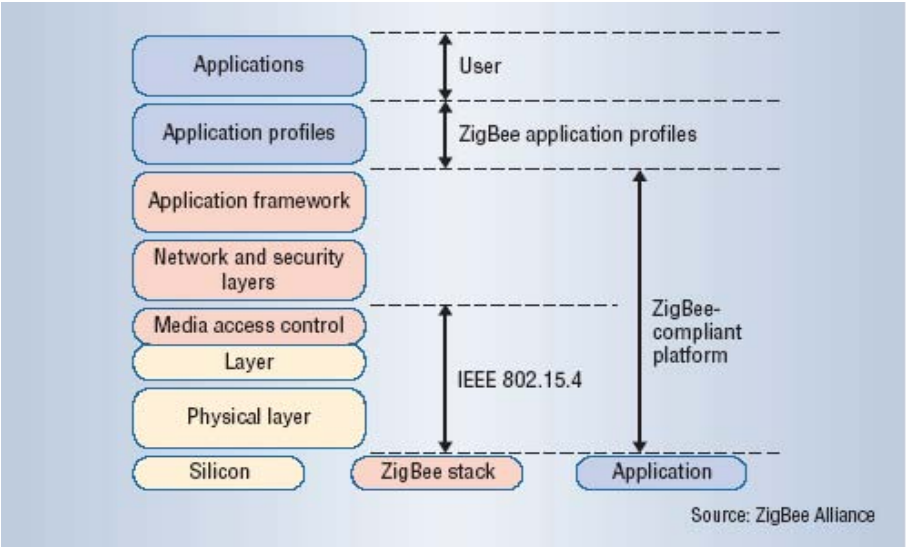

Figure 5. IEEE 802.15.4 and ZigBee working model (Le, 2005).

I. IEEE 802.15.4 STANDARDS AND THE PHYSICAL LAYER

The IEEE 802.15.4 standard defines the physical layer in all ZigBee devices. The PHY is responsible for data transmission and reception by using certain radio channel and specific modulation and spreading technique (Koubaa, 2005). The IEEE 802.15.4 standard specifies two PHYs that represent three operational frequency bands. These three bands include: 868 MHz (used in Europe), 915 MHz (used in America), and 2.4 GHz (used worldwide) (Scott, 2005). The 868 and 915 MHz bands are in one PHY while the 2.4 GHz band is in the second PHY. There is a single channel between 868 and 868.8 MHz, 10 channels between 902 and 928 MHz, and 16 Channels between 2.4 and 2.4835 GHz (Koubaa, 2005).

The three operating frequency bands are good choices for ZigBee low cost sensor networks because they are unlicensed and the spectrum is widely available. Table 2 below quickly outlines the PHY with its operating characteristics.

PHY	Frequency Band	Channel Numbering	Bit Rate
868/915 MHz	868-870 MHz 902-928 MHz	0 1 to 10	20 kb/s 40 kb/s
2.4 GHz	2.4-2.4838 GHz	11 to 26	250 kb/s

Table 2. Frequency Bands and Data Rate.

As Table 2 demonstrates, data rate increases as the frequency band increases. In low data rate transmissions, better sensitivity and larger coverage area are provided. Likewise, higher data rate provides higher throughput, and lower latency. In addition, lower frequencies have lower propagation losses thus they are more suitable for longer

transmission range. All the frequency bands in the PHY are based on the Direct Sequence Spread Spectrum (DSSS) spreading technique.

1. Responsibilities of the Physical Layer

In the 802.15.4 standard, the physical layer is responsible for five specific tasks (Koubaa, 2005). The first task is the activation and deactivation of the radio transceiver. The radio transceiver operates in the following three modes: transmitting, receiving, or sleeping. When the PHY receives a request from the MAC sub layer, the radio transceiver is turned ON or OFF. The second responsibility of the PHY is energy detection (ED) within the current channel. The PHY estimates the amount of energy in the received signal power within the bandwidth of a channel. The ED is used by the network layer to channel select and to determine if the channel is busy or idle. The third task of the PHY is link quality indication (LQI). The LQI is measured by the PHY to determine the strength and quality of a received packet. Another responsibility of the PHY is clear channel assessment (CCA). The purpose of the CCA is to report the activity state of the medium which is either busy or idle. The CCA performs this task by using three different operational modes:

- Energy Detection Mode: CCA reports a busy medium if the detected energy is above the ED threshold.
- Carrier Sense Mode: CCA reports a busy medium if it detects a signal with the modulation and spreading characteristics of IEEE 802.15.4.
- Carrier Sense with Energy Detection Mode: CCA reports a busy medium if it detects a signal with the

modulation and the spreading characteristics of IEEE 802.15.4 and with the energy that is above the ED threshold.

The fifth and last responsibility of the PHY is channel frequency selection. With 27 different channels provided by the IEEE 802.15.4, the PHY must be able to select the specified channel that is requested by a higher layer. This task and the other four mentioned above help the PHY to transmit and receive data.

J. THE MEDIUM ACCESS CONTROL (MAC) SUB LAYER

In addition to the PHY, the IEEE 802.15.4 standard defines the medium access control sub layer for all ZigBee devices. The MAC sub layer protocol serves as the interface between the PHY and the higher layer protocols (refer to Figure 6). The functions of the MAC include synchronization, frame validation, acknowledged frame delivery, association, and disassociation (Ding, 2005). Also, the MAC controls the access to the radio channel by employing the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism (Ding, 2005). CSMA/CA is a network contention protocol that listens to the network in order to avoid collision (Wikipedia.com, 2006). The basic mechanism of CSMA/CA is as followed:

When a node wants to transmit a packet, it has to check to ensure that the channel is clear (i.e., no other node is transmitting at the same time). If the channel is busy, then the node waits for a randomly chosen period of time to transmit again. If the channel is free, then the node is allowed to transmit. The implementation of CSMA/CA by the MAC sub layer prevents collisions and allows the packets to be transmitted quicker. Reducing collisions is

a major concern to ZigBee devices since collisions are more likely to occur in low data rate networks (Koubaa, 2005).

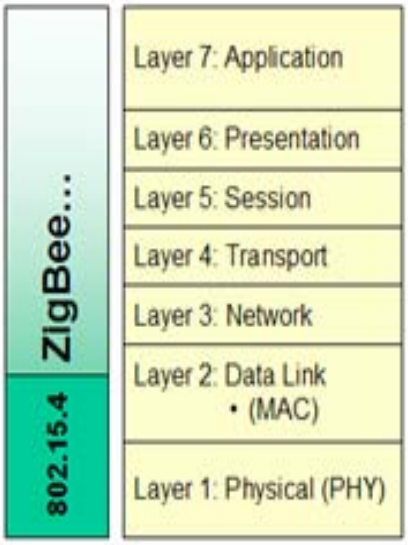

Figure 6. OSI 7-Layer Model.

K. 802.15.4 NETWORK TOPOLOGIES

The ZigBee Alliance adopted the 802.15.4 standard for its PHY and MAC layer. However, ZigBee is responsible for defining the network, security, and application framework profile layers. The ZigBee network layer supports three types of networking topologies which include star, mesh, and cluster tree (Streeton, 2005). The star topology is most common and provides for very long battery life operation. The mesh topology (also known as peer to peer) is used when the operators want high levels of reliability and scalability. The last type of network topology is the cluster tree which is a combination of the star and mesh topology. The cluster tree topology incorporates the advantages of the other two topologies to achieve a high level of reliability and long operating time.

1. Star Topology

In the star topology (see Figure 7), one node operates as the Personal Area Network (PAN) coordinator in which all communications among the nodes is channeled through. The node that is the PAN coordinator must be capable of communicating with the other devices in the network. This capability is also used to describe the PAN coordinator node as a Full-Function Device (FFD). On the other hand, a Reduced-Function Device (RFD) can only communicate with the FFD.

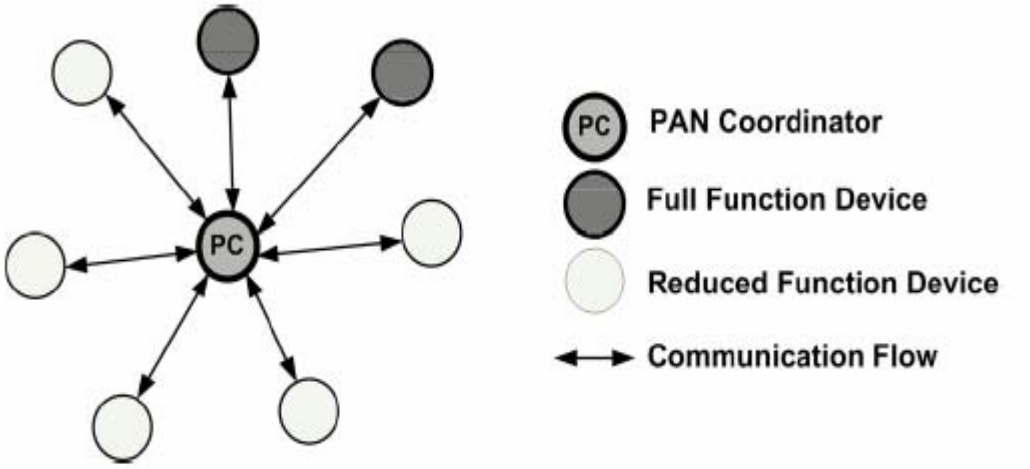

Figure 7. Star topology (Koubaa, 2005).

The star topology is a centralized network in which all devices (whether FFD or RFD) join in the network must send their data to the PAN coordinator. After receiving the data, the PAN coordinator transmits them to the appropriate device. Since the PAN coordinator has multiple tasks in this topology, its power consumption is much higher than the other devices and may require mains

powered. Unlike the PAN coordinator, the other devices have to receive and transmit for short periods of time and can operate using battery power.

2. Mesh Topology

The second type of topology that is supported by the ZigBee network layer is the mesh topology. The mesh topology is a decentralized network where all devices can communicate with any other devices if they are within their communicating range. The mesh topology also has a PAN coordinator which is selected by being the first FFD to communicate on the channel. The major advantages of the mesh topology are that it provides greater networking flexibility and reliability. These advantages are achieved by establishing multiple paths to route data from one device to another device.

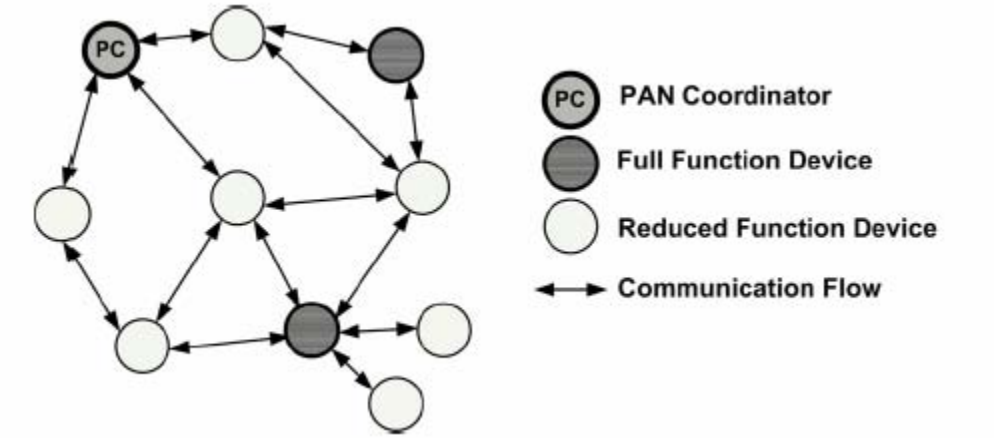

Figure 8. Mesh topology (Koubaa, 2005).

3. Cluster Tree Topology

The third type of ZigBee networking topology is the cluster tree topology. The cluster tree is a modification of the mesh network in which most of the devices are FFDs. The cluster tree is formed by having a PAN coordinator

establishing itself as the Cluster Head (CLH) with a cluster identifier (CID) as zero. A neighboring cluster that wants to join in the network may send a request to the PAN coordinator. Once the neighboring cluster joins the PAN coordinator, the cluster identifies itself as CLH1 with the number one as the CID. The PAN coordinator serves as the parent node for the two clusters, receiving data and transmitting beacons. The biggest advantage of the cluster tree topology is that the network can increase with additional clusters thus extending the geographical range of the network.

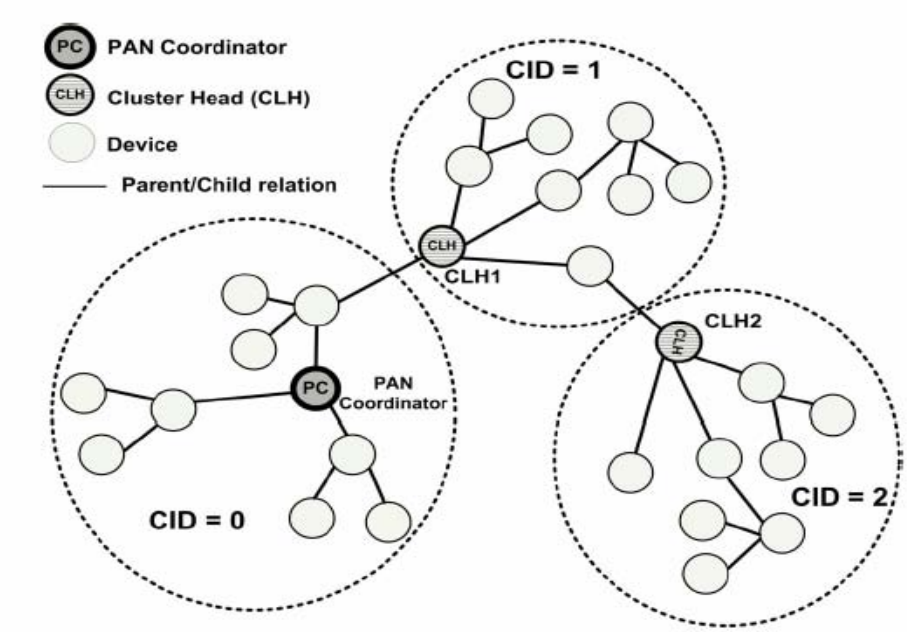

Figure 9. Cluster tree topology (Koubaa, 2005).

L. SUMMARY

The focuses of Chapter II include sensor nodes, wireless sensor network, IEEE 802.15.4 standard, and ZigBee technology. The chapter provides an introduction to sensor nodes and wireless sensor networks. It describes the

qualities of sensor nodes and lists the capabilities and limitations of WSNs. The second half of the chapter talks about the IEEE 802.15.4 and the ZigBee WSN standards. The discussion on the 802.15.4 and ZigBee standards include WPAN, PHY layer, MAC sub layer, and the ZigBee network topologies. Chapter III will focus on the military applications of WSNs.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MILITARY APPLICATIONS OF WIRELESS SENSOR NETWORKS

A. INTRODUCTION

The emergence of WSNs has opened up new opportunities and applications. Until the development of ZigBee standards, there was little interest in the utility of sensors and control devices. The ZigBee standards open the market for devices that require low bandwidth and low data rate. ZigBee wireless sensors are designed to be reliable, low energy consumption, and with the added benefit of being low cost. Similar to the business industry, the military has taken an interest in the applications of WSNs. Since WSN technology is recent, military applications have not been fully explored or utilized. However, with increased research and exposure to WSNs, the military will find many useful applications that will enable its fighting forces to win the war.

B. MILITARY OBJECTIVES

Technology is an integral component for the war fighters in today’s military. WSNs can be the far reaching eyes and ears for both the soldiers on the battlefields and the commanding officers who are away from the front. The military seeks to capitalize on WSN technology, in particular, low data rate and low bandwidth sensors. The applications of WSNs can be seen as a revolutionary change that can affect the way wars are fought.

1. Benefits of WSNs

The applications of WSNs provide the military with three significant benefits. These include establishing overarching situational awareness, providing a common operational picture across all echelons of the military,

and enhancing decision-making for military leaders. To achieve these objectives, the military must look to the deployment of multiple networks consisting of low cost sensors that can see and hear where the other technology cannot.

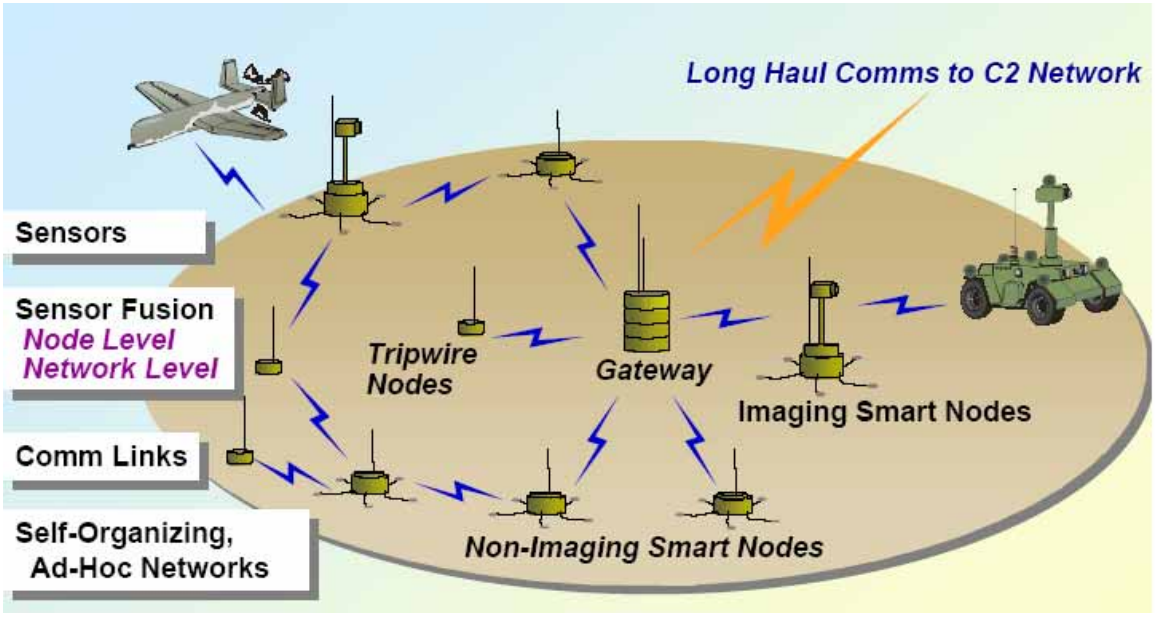

Figure 10. A Sensor Network (Eicke, 2002).

2. Military Criteria for WSNs

In order for the military to deploy effective networks of sensors, the military must establish criteria for the sensors. Three criteria have already been mentioned: low cost, low data rate, and low bandwidth. In addition to these criteria, wireless sensors must be capable of sensing information with high fidelity. For the military, the sensors are used to target people or objects of interest, detect potential hostile threats, and assess battle damages. The information must be captured with accuracy by the sensors. Another criterion is that the sensors are

integrated with other sensors to produce a complete and accurate picture of the environment. Integration will allow a network of sensors with various capabilities to relay different information on a particular target. In addition to integration, wireless sensors must have a high degree of sustainability. When sensors are deployed on the battlefield, redundancy is vital so that no one sensor can bring down the network. The last criterion that the military looks for in the wireless sensors is low complexity and ease of use. In order for the sensors to be operational on the field, any soldier with minimum training can operate them. To be effective tools, sensors must be easy to handle for war fighting operators. These criteria are required by the military due to the nature of its missions and the potential risks that are associated with them.

The military does not need to look far for technology that meets the criteria that are mentioned in the above paragraph. Wireless sensor networks are ideally designed for military operations.

C. ADVANTAGES OF WSN TECHNOLOGY

1. Self-organizing, Ad-hoc Network

WSNs can operate in a self-organizing, ad-hoc network. In the mesh topology, sensors can form their own connections with other sensors. In addition, when one sensor in the network is destroyed or fails to transmit and receive, the other sensors can easily reconnect with their nearest neighbors to establish a link with the base station node. Self-organizing, ad-hoc network is also useful for the military because that characteristic enables the military to implement various deployment mechanisms.

Sensors can be individual deployed by hands or they can be released over the desired operating area via low flying airplane or helicopter. The autonomous nature of WSNs makes them highly deployable and dependable in maintaining the sensor network.

2. Low Data Rate

Another quality of WSN sensors is that they operate in a low data rate environment ranging from 30 kbps to 250 kbps. The need for information by the military has increased the demand for bandwidth. Satellite communications, real-time imaging, and video conferencing have constrained the available bandwidth that the war fighters need to operate. ZigBee sensors are the solutions that allow operators to capture relevant information with little bandwidth.

3. Low Complexity and Low Cost

In addition to operating at a low data rate environment, WSN sensors are also expected to be low complexity and low cost. Low complexity provides the benefit of high durability. Less complex sensors do not required much circuitry and are less prone to failure. In addition, the sensors incorporate technology which enables the hardware designers to make the sensors smaller. Currently, WSN sensors can be the size of a small quarter. The technology has not yet progressed toward the point where WSN motes are the size of dust. Small and durable sensors are advantageous when it come to military applications. The low cost aspect of sensors also allows the military to deploy large quantity of sensors thus producing robust networks. Affordable sensors with low technology overhead make ZigBee WSNs the optimal choice for the military.

D. TYPES OF SENSORS

To meet its objectives of achieving situational awareness, acquiring a common operational picture, and enhancing decision-making, the military can deploy wireless networks comprising of various types of low cost sensors. The strength of the networks is the aggregation of the differing sensors to form a complete picture of the environment. The military has many types of sensors that it can utilize to meet these objectives. These sensors are discussed below.

1. Acoustic/Seismic Sensors

These sensors provide 360-degrees of non-line-of-sight (NLOS) monitoring. They are used to classify and identify targets of interest (vehicles, helicopters, artillery, and gunfire). In addition, the sensors can provide line-of-bearing (LOB) to a target that has been detected. With multiple acoustic sensors, triangulation can be used to locate detected targets. Figure 11 illustrates examples of acoustic and seismic sensors.

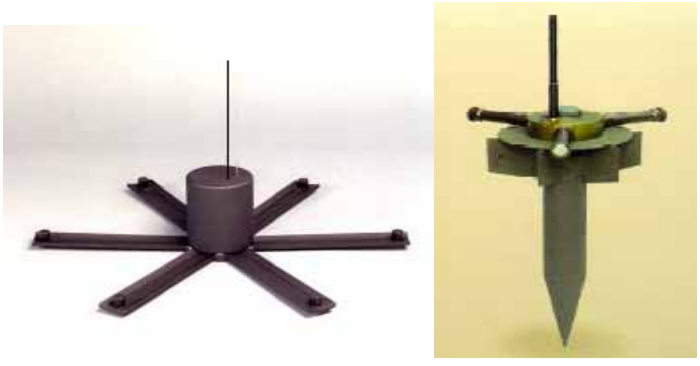

Figure 11. Acoustic/Seismic Sensors (Eicke, 2002).

2. Magnetic Sensors

Similar to the acoustic sensors, magnetic sensors also provide 360-degrees of NLOS monitoring. They are used to detect vehicles and small arms. The Crossbow MSP410CA is an example of mote which includes a magnetic sensor. Depending on the type of object, its size, and its ferrous content, the mote can detect an object at a range of 18 meters.

Figure 12. MSP410CA Mote (xbow.com, 2006).

3. Infrared (IR) Sensors

IR sensors are the third type of sensors that are available to obtain and deploy in a wireless network. Similar to the other two sensors mentioned above, IR sensors are low cost, low power, and low complexity. In a network suite of sensors, the IR sensors are excellent resources to identify targets. The acoustic and magnetic sensors can be deployed as early warning devices. Once the targets are acquired, the IR sensors can provide additional details to make target identification easier for the military war fighters.

Figure 13. IR Sensor (Eicke, 2002).

E. APPLICATIONS OF WSNS

WSNs play an important role in the military in terms of command, control, communications, computing, intelligence, surveillance, and reconnaissance (C4ISR). To achieve military superiority, the soldiers on the battlefield must be able to access vital information. The soldiers shouldn't be limited by voice communications or point-to-point long range communications to get their information. Both forms of communications have weaknesses that can endanger the modern war fighters. WSNs are means whereby soldiers can communicate with each others and obtain information effectively.

1. Monitor Troop and Equipment

WSNs can be used by the military to monitor friendly forces and equipment. Small wireless sensors are attached to soldiers, vehicle, and equipment to monitor and report their current condition. This information is collected by the sink nodes and is forwarded to upper command where decision-making can be facilitated.

2. Perimeter Surveillance

Another use of a WSN by the military is for surveillance of perimeters and critical passage points. Friendly forces can cover their defensive perimeters with sensor networks to detect unauthorized entry by the opposing forces. In addition, the sensor networks can be used along critical roads to detect enemy's movements.

Figure 14 below is an illustration of a sensor attached to a work cone for the purpose of monitoring the roads and perimeter. The sensor is capable of passive infra-red detection with a range of 25 to 80 feet and magnetic detection with a range of 25 to 50 feet. The sensor attaches to the work cone non-discretely and requires little interaction from the user.

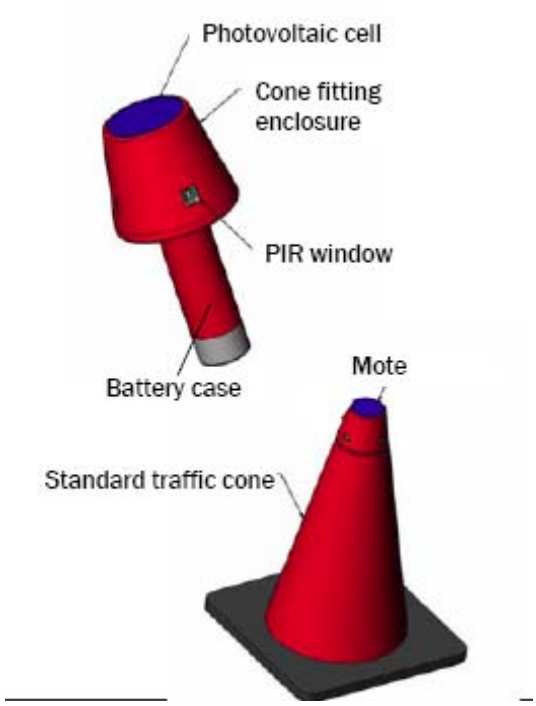

Figure 14. Sensor Cone (xbow.com, 2006).

3. Sniper Location

The targeting of snipers is another application of a WSN that is currently being used by the military. Acoustic sensors are used to triangulate and locate the source of the shock wave and blast produced by the snipers firing their weapons. The sensor nodes detect the shockwave and muzzle blast from the enemy. That information is forwarded by the nodes to the base station where the sniper location is determined. The performance of this system has been tested by Crossbow and the results are good. The average accuracy of locating the shooter is 1 meter and the latency is only 2 seconds (xbow.com, 2006).

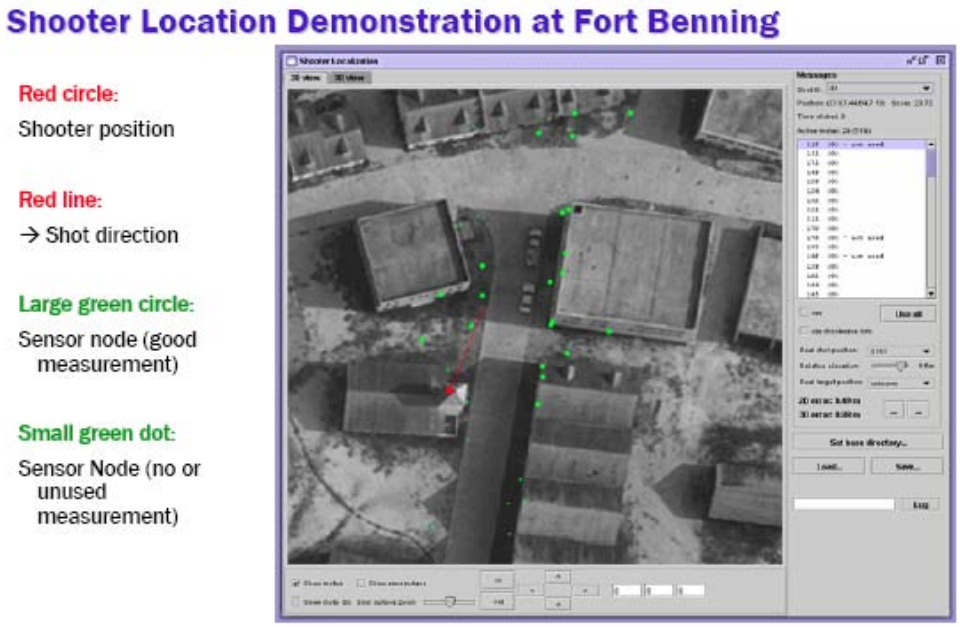

Figure 15. Sniper Location (xbow.com, 2006).

F. CONCLUSION

In today's military, information and knowledge play a vital role in accomplishing the mission. To be successful on the battlefields, the military must expand its horizon to acquire information. From the acquisition of information, knowledge can be achieved. With that knowledge, both the soldiers and commanders are able to carry out their tasks to the fullest of their abilities. WSNs are the tools that can help the military reach that goal. With the application of these tools, the military can extract and exchange information both locally and over long distance.

IV. OVERVIEW OF CROSSBOW MSP410CA MOTE SECURITY SYSTEM

A. INTRODUCTION

This chapter discusses the Crossbow hardware and software that are used in this thesis. The chapter focuses mainly on the Crossbow MSP410CA Mote Security System as the hardware and the MOTE-VIEW client as the software. However, other Crossbow hardware and software are also presented in this chapter.

B. OVERVIEW OF CROSSBOW HARDWARE PRODUCTS

Crossbow is a leading provider of WSN equipment (xbow.com, 2005). It was founded in 1995 and is headquartered in San Jose, California. Crossbow creates and deploys small wireless sensing devices for environmental, agricultural, industrial monitoring and control, building automation, security, and asset tracking applications (xbow.com, 2006).

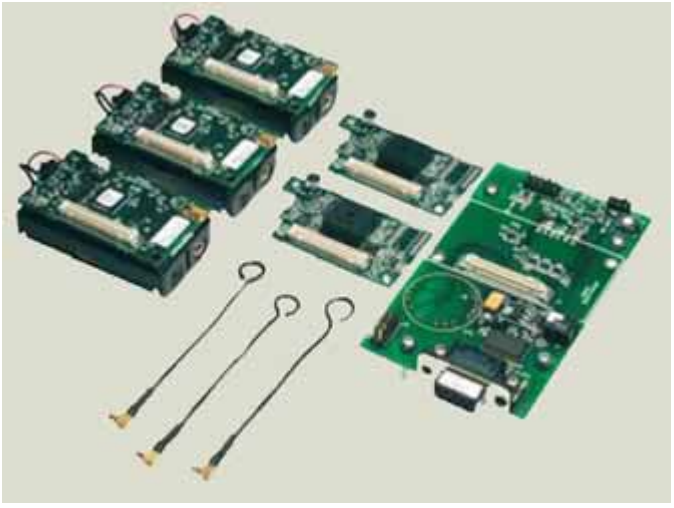

Figure 16. Crossbow process/radio boards.

1. Crossbow Motes

Crossbow provides a wide range of processor/radio boards, which are more commonly known as motes. The motes sold by Crossbow were originally developed by the University of Berkeley. Crossbow offers several types of motes including MICA, MICA2, MICA2DOT, and MICAz. Table 3 lists the four different types of motes and their respective characteristics. The table shows that the motes may have different qualities, but they all share one common trait. That commonality is the low power consumption of the motes which contributes to the long battery life.

Mote Hardware Platform		MICAz	MICA2	MICA2DOT	MICA
Models (as of August 2004)		MPR2400	MPR400/410/420	MPR500/510/520	MPR300/310
MCU	Chip	ATMega128L			ATMega103L
	Type	7.37 MHz, 8 bit		4 MHz, 8 bit	4 MHz, 8 bit
	Program Memory (kB)	128			
	SRAM (kB)	4			
Sensor Board Interface	Type	51 pin		18 pin	51 pin
	10-Bit ADC	7, 0 V to 3 V input		6, 0 V to 3 V input	7, 0 V to 3 V input
	UART	2		1	2
	Other interfaces	DIO, I2C		DIO	DIO, I2C
RF Transceiver (Radio)	Chip	CC2420	CC1000		TR1000
	Radio Frequency (MHz)	2400	315/433/915		433/915
	Max. Data Rate (kbits/sec)	250	38.4		40
	Antenna Connector	MMCX		PCB solder hole	
Flash Data Logger Memory	Chip	AT45DB014B			
	Connection Type	SPI			
	Size (kB)	512			
Default power source	Type	AA, 2×		Coin (CR2354)	AA, 2×
	Typical capacity (mA-hr)	2000		560	2000
	3.3 V booster	N/A			✓

Table 3. Specifications of Crossbow motes (Tingle, 2005).

2. Radio

One component of the Crossbow motes is the radio. The radio allows a mote to transmit and receive data. It is the link between the base station and the deployed nodes. The type of radio that Crossbow employed in its MICA and

MICA2 motes is the Chipcon CC1000 RF Transceiver. One key feature of the CC1000 RF Transceiver is that it requires low power for operation. To transmit a package, the transceiver requires only 9.1 mA of power. Another feature of the transceiver is that it uses PSK modulation with a data rate of about 76.8 kbps (Chipcon.com, 2006).

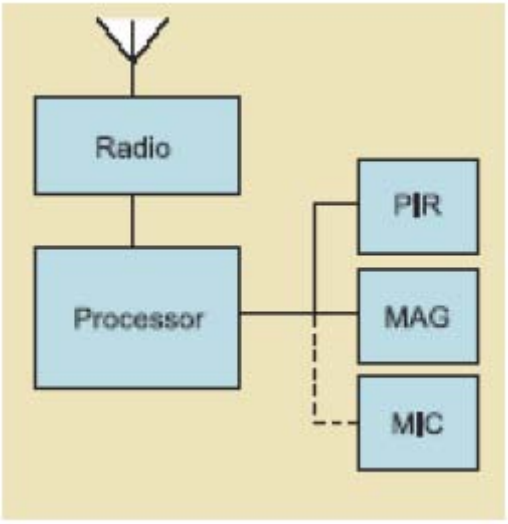

Figure 17. Mote's Basic Block Diagram, MSP410CA Datasheet (xbow.com, 2006).

3. Microcontroller

Another key component of the motes is the microcontroller, which is also known as the processor. As indicated from Table 3, most of Crossbow motes utilize the Amtel ATMega 128L microcontroller. The microcontroller has a 7.3728 MHz clock, 128 kB of flash memory, 4 kB of Static Random Access Memory (SRAM), and two Universal Asynchronous Receive and Transmit (UARTs). The microcontroller is connected to the external flash and the 64 bit Serial ID number. It is typically powered by two AA batteries and requires an operating voltage of 2.2 V (Tingle, 2005).

4. Crossbow MSP410CA Mote Security System

a. Overview

From the list of available Crossbow motes, this thesis focuses on the implementation and testing of the MSP410CA Mote Security System. The MSP410CA system consists of eight simple to deploy MICA2 motes (MSP410CA) and one base station mote (MBR410CA). The eight MSP410CAs are powered by two AA batteries and are encased in a heat reflective enclosure. They are deployed along a road or perimeter in order to sense and track people or vehicles. Information that is detected by the MSP410CA motes is transmitted to the MBR410CA base station mote. The MBR410CA interfaces with a laptop or PC and allows the users to view the network and data collected by the MSP410CA motes. Figure 18 illustrates the components of the MSP410CA Mote Security System.

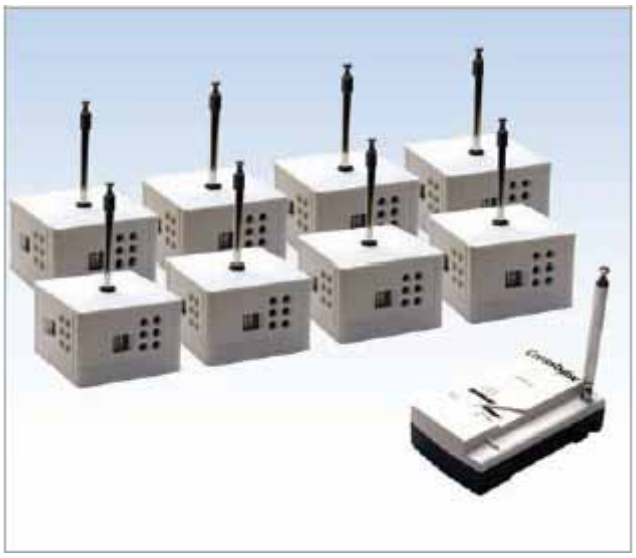

Figure 18. Crossbow MSP410CA Mote Security System.

b. Deployments of MSP410CA Mote Security System

The MSP410CA Mote Security System is designed for security applications. Some of these applications include remote border security, perimeter protection, intrusion detection, and building occupancy monitoring. To set up the MSP410CA system for a security application, the motes are deployed in a perimeter or grid pattern. Figure 19 provides an illustration of a perimeter deployment around a building. The figure also shows how the motes are oriented and spaced apart according to Crossbow specifications.

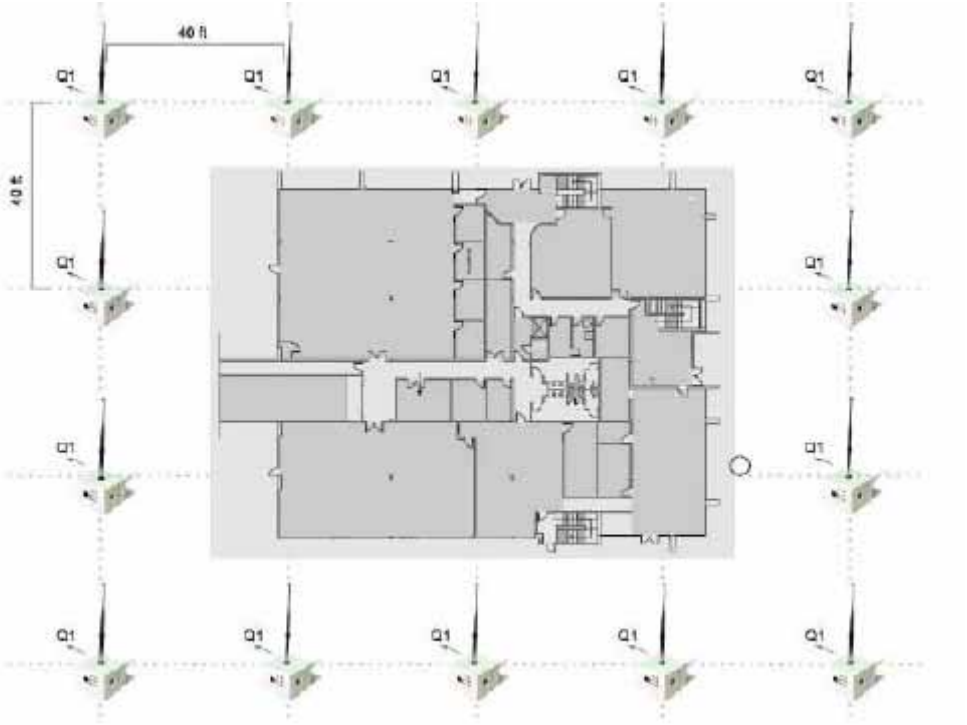

Figure 19. MSP410CA Perimeter Monitoring (Crossbow User's Manual, 2005).

In addition to the perimeter deployment, the MSP410CA system can also be deployed in a dense grid. The Crossbow user's manual provides an illustration of the

dense grid with its recommended distances and orientation. The purpose of the dense grid is to provide complete coverage over the area of interest. The distances in both the perimeter and dense grid deployments are restricted by the average sensor's effective distances and not by the communication ranges of the motes. Therefore, the distances between motes can be increased if the user doesn't require complete area coverage. In the deployments of the MSP410CA system, the user has to consider the placement of the motes to achieve the desired balance between sensor coverage and area coverage.

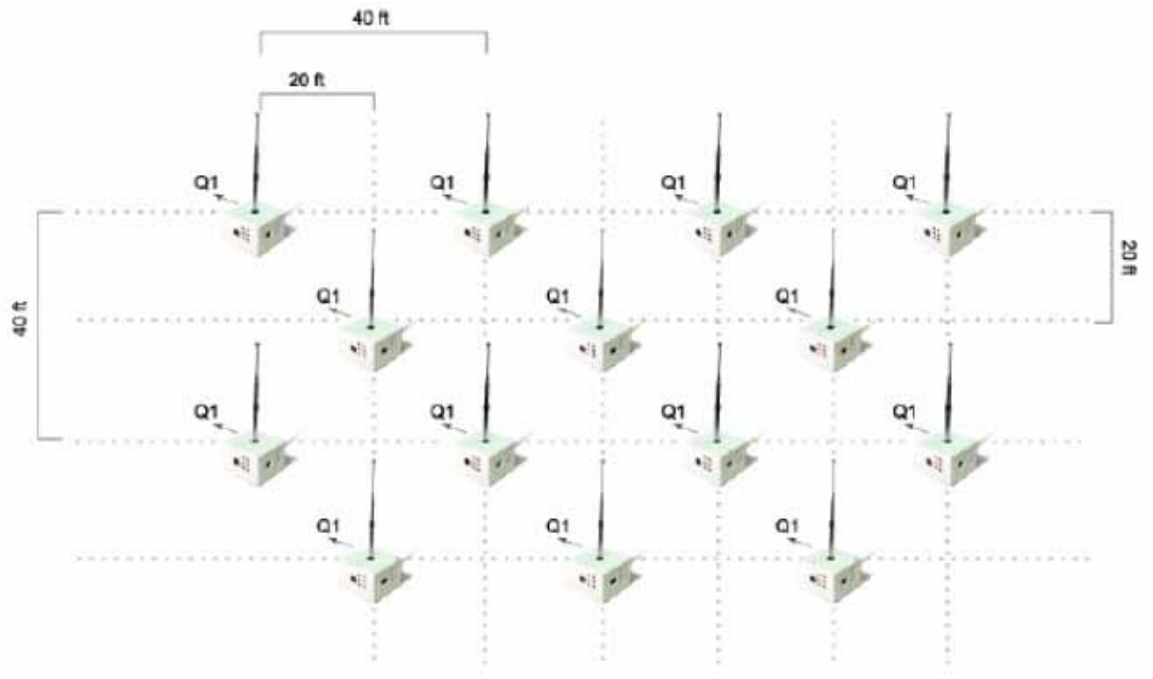

Figure 20. MSP410CA Dense Grid Monitoring (Crossbow User's Manual, 2005).

c. Components of MSP410CA System

The MSP410CA Mote Security System consists of two components: the MSP410CA motes and the MBR410CA base station. The MBR410CA base station is discussed later in

the chapter. Crossbow provides eight MSP410CA motes in its security system kit. The eight motes are the heart of the surveillance system responsible for sensing their environment and forwarding that information to the base station. In addition, the motes are responsible for forming the wireless mesh ad-hoc network and maintaining that network if one of the motes is damaged or lost power.

The motes used in the MSP410CA security system are MICA2. MICA2 are classified into three models based on their RF frequency band. These models include the MPR400(915MHz), the MPR410(433MHz), and the MPR420(315MHz). The MSP410CA system uses the MPR410 model for its MICA2. Figure 21 provides an illustration of the MICA2.

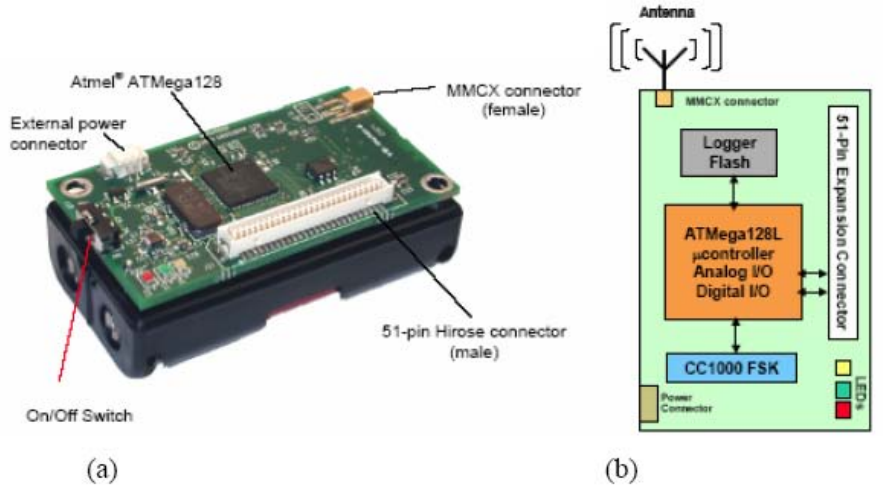

Figure 21. (a)MICA2 without antenna, (b)MICA2 block diagram (Crossbow User's Manual, 2005).

The MICA2 is composed of two components: the radio and the microcontroller. The MICA2 uses a Chipcon CC1000 radio with an operating frequency at 433MHz. The radio is able to transmit at an effective baud rate of 19.2

kbps (Crossbow, 2005). The other component of the MICA2 is the processor which uses the Amtel Atmega 128 microcontroller. The microcontroller is the heart of the mote which controls all of its functions.

d. MSP410CA (mote) Magnetic Sensor

The MSP410CA motes are the sensing eyes and ears of the surveillance system. Some of the features that have been incorporated into the MSP410CAs by Crossbow include magnetic and passive infrared sensors (PIR). The MSP410CAs have a two axis magnetic field sensor that detects perturbations in the local magnetic field. Depending on an object size and its ferrous content, the magnetic field sensor can detect the object at the maximum range of 18 meters. Table 4 below shows the magnetic sensor specifications for the MSP410CA motes.

Parameter	**Typical value**	
Bridge resistance	1100 ohms	
Field range	± 6 gauss (Earth's field = 0.5 gauss)	
Sensitivity	1 mV/V/gauss	
Linearity error (best fit straight line)	± 1 gauss	0.05% FS
	± 3 gauss	0.4% FS
	± 6 gauss	1.6% FS
Bandwidth	DC to 5 MHz	
Noise Density	50 nVsqrt Hz @ 1kHz	
Resolution	120 µgauss @ 50 Hz BW	
Storage Temperature	-55°C to 175°C	

Table 4. Magnetic Sensor Specifications for MSP410CA Mote (xbow.com, 2006).

e. MSP410CA (mote) Passive Infrared Sensor

In addition to the magnetic sensor, the MSP410CA motes have passive infrared sensors that are used to detect dynamic changes in the local thermal radiation environment. The MSP410CA motes are designed with four separate PIR sensors that are arranged orthogonally to provide 360-degree of coverage in the horizontal plane. A lens enhances the sensor's capabilities by generating a vertical field of view ±15 degrees and ±45 degrees in the horizontal field. The four PIR sensors give the MSP410CA motes the "Quad Detect" capability that enables the identification of initial object vector. In addition, the Quad Detect can identify an object's subsequent movement and direction. The PIR sensors can detect people and vehicles at a range of eighty feet (Xbow.com, 2006). Table 5 below lists the specifications of the PIR sensors found in the MSP410CA motes.

Specifications - Performance	Value	Comments
Optical wavelength	5 µm to 14 µm	
Optical bandwidth	0.01 Hz to 15 Hz	
Field of view vertical	± 15° °	
Field of view horizontal	± 45	
Storage temperature	-55°C to +125°C	
Range for human detection	30' to 40'	For Motes height ≈ 3' off the ground Outdoor air temperature ≈ 7°C.
Range for cars detection	50' to 60'	
Range for large tracks detection	70' to 80'	

Table 5. PIR Sensor Specifications for MSP410CA Mote (xbow.com, 2006).

5. MBR410CA Base Station Mote

The first component of the MSP410CA Mote Security System consists of the MSP410CA motes. The second component of the system is the MBR410CA base station mote. The base station is an important wireless sensor network interface with other systems. The function of the MBR410CA is to aggregate sensor network data onto a laptop or PC. This task is accomplished through the utilization of the 433 MHz MICA2 processor/radio board and the MIB510 serial gateway. These two components of the base station are connected together and housed inside a protective enclosure (refer to Figure 22). In addition, the base station also has the function of reprogramming the deployed motes.

Figure 22. MBR410CA Mote.

C. OVERVIEW OF CROSSBOW SOFTWARE PRODUCTS

1. TinyOS

At the heart of the Crossbow hardware is the small yet powerful operating system that is referred to as Tiny Micro Threading Operating System (TinyOS). TinyOS is an open source operating system designed for WSN. It is a component based operating system architecture that enables

rapid innovation and implementation while minimizing code size (Rajaravivarma, 2003). It is also an event-driven operating system framework that enables fine grained power management and facilitates scheduling flexibility (Tinyos.net, 2006). TinyOS runs the sensor hardware and the communications network. It also makes sensor measurements, routes measurement data, and controls the power dissipation within the hardware (Rajaravivarma, 2003).

TinyOS has three software components: command, event, and tasks. Commands are non-block requests made to initiate action by a lower level component. Events notify high level actions that have occurred and call low level commands. Lastly, tasks are used for long running computations that are initiated by events (Rajaravivarma, 2003).

2. XServe Software

Crossbow uses the open source TinyOS as the operating system for its hardware. In addition, Crossbow has developed its own set of software to interface with the server and client. One software designed by Crossbow is XServe. XServe is a middleware that connects WSN to the IT infrastructure and to the internet. It is the gateway that connects the physical world to the internet. Its key features include: data logging service to file or database, data forwarding via TCP/IP sockets, web-page output, alert detection, manages mote network upgrade, and aggregates network health messages (Xbow.com, 2006).

3. Surge Network Viewer

The second software that is used by Crossbow is Surge Network Viewer (Surge-View). Surge-View is used to monitor a sensor network and analyze mesh network performance. The key features of Surge-View include: automatic discovery and network configuration, viewing of sensor network topology, logging and viewing of network statistics, and graphical tool for viewing logged data (Buschmann, 2005).

4. Mote-View Client Software

The third and last Crossbow software is Mote-View Client software which is a user interface application for remote monitoring of the sensor network. This client server allows a user to graphically view the deployed wireless sensors in the field. The purpose of the software is to simplify deployment and monitoring for the users. It provides an easy mean of logging wireless sensor data to a database, analyzing and plotting sensor readings. The key features of Mote-View include: historical and real-time charting, topology map visualization, network visualization, sensor-value gradient visualization, data export capability, and printed report generation (Xbow.com, 2006).

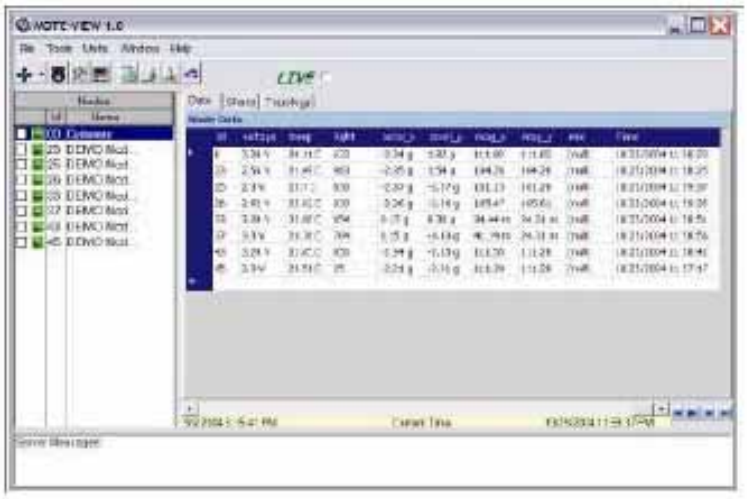

Figure 23. Screenshot of Mote-View Data View (Crossbow User's Manual, 2005).

Mote-View supports the Crossbow MICA family of WSN hardware, including the MICA2, MICA2DOT, and MICAz. It is used in the MSP410CA Mote Security System to check systems topology and network connections. Mote-View is an invaluable software tool that allows the user to graphically interface with the WSN devices.

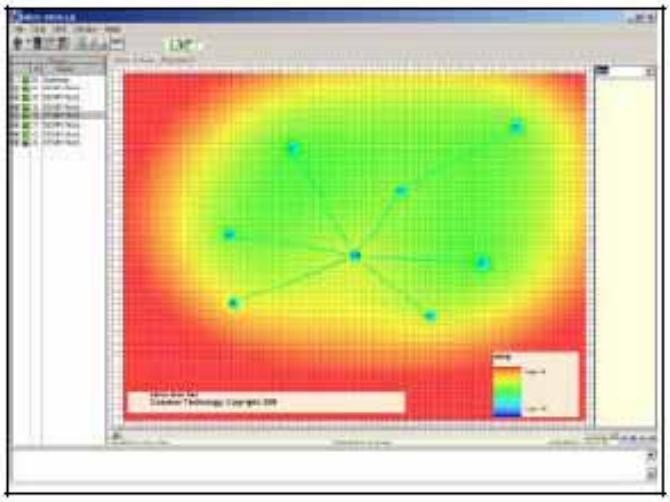

Figure 24. Screenshot of Mote-View Topology View (Crossbow User's Manual, 2005).

THIS PAGE INTENTIONALLY LEFT BLANK

V. DEPLOYMENT OF MSP410CA MOTE SECURITY SYSTEM

A. INTRODUCTION

The chapter begins with a description of a WSN surveillance system developed at NPS. Afterward, the chapter describes the test scenario of the system. Finally, the chapter ends with the observations from the test results.

B. NPS SURVEILLANCE SYSTEM

The acquisition of timely information is an important issue for the military. WSNs are the means whereby the military can acquire relevant information, gain control of the operational environment, and improve tactical situational awareness. The Naval Postgraduate School (NPS) and the Royal Thailand Armed Forces are currently conducting a research project that addresses that issue. The Coalition Operating Area Surveillance and Targeting System (COASTS) project uses wireless technologies to obtain and display information from both air and ground sensors. The various types of sensors used by COASTS are deployed on air balloons, Unmanned Aerial Vehicles (UAVs), and portable and fixed ground-based sensors. The data received by these sensors are transmitted to a Command and Control center via WLAN technologies. The COASTS project integrates different types of networks to produce a complete picture of the operational environment.

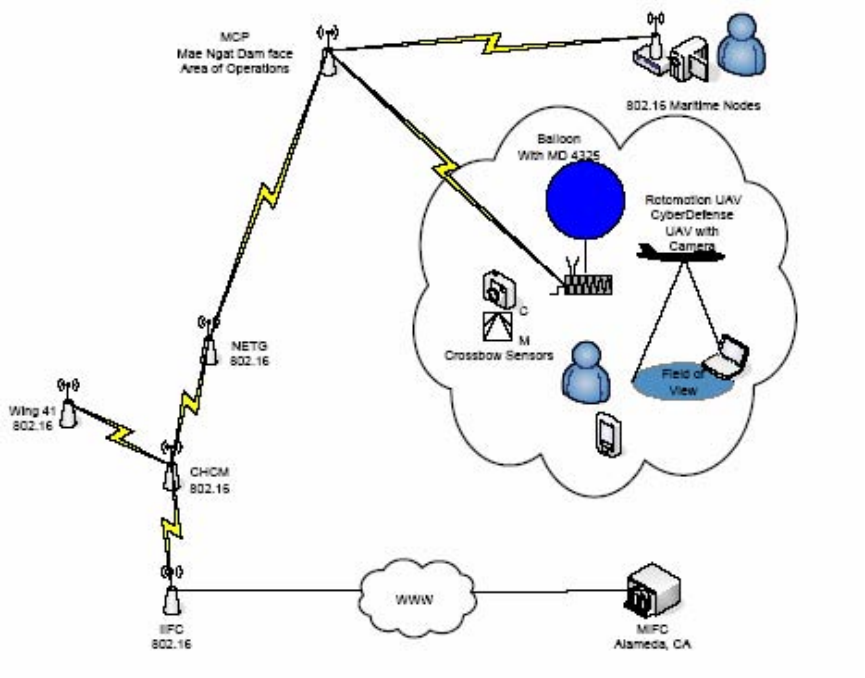

Figure 25. COASTS Topology View (COASTS OPORD, 2006).

The objectives of COASTS are to support research and development on WSNs, conduct operational testing on the wireless equipments, and validate the wireless technologies. These wireless technologies include 802.11, 802.16, 802.15.4, satellite communications, portable computing devices, air sensors, and fixed ground sensors. The successful incorporation of these technologies allows COASTS to meet its mission objectives. Through the application of WSN, COASTS hopes to accomplish its seven principal objectives. These mission objectives include:

- Provide force protection
- Conduct tactical reconnaissance
- Provide internal defense to host nation
- Combat terrorism
- Provide assistance to civil affairs activities

• Assist in the counter-proliferation of Weapons of Mass Destruction

• Defend one’s information systems

With these seven mission objectives in mind, COASTS creates a wireless communication network capable of interlinking different technologies to provide an accurate operational picture.

One technology that is incorporated by COASTS is the Crossbow MSP410CA Mote Security System. The purpose of the Crossbow security system is to serve as an unattended grid to detect, identify, and track suspicious people and vehicles. Once the Crossbow sensors detect an object, a surveillance camera is activated to assist in the visual identification of the object. In the COASTS project, information that is collected by the low data rate sensors is forwarded to the Command and Control base station via the 802.11 infrastructure. The Crossbow sensors create their own network. However, the information from that network is shared via the WLAN. Figure 26 illustrates the deployment of the sensors along a road to monitor suspicious traffic.

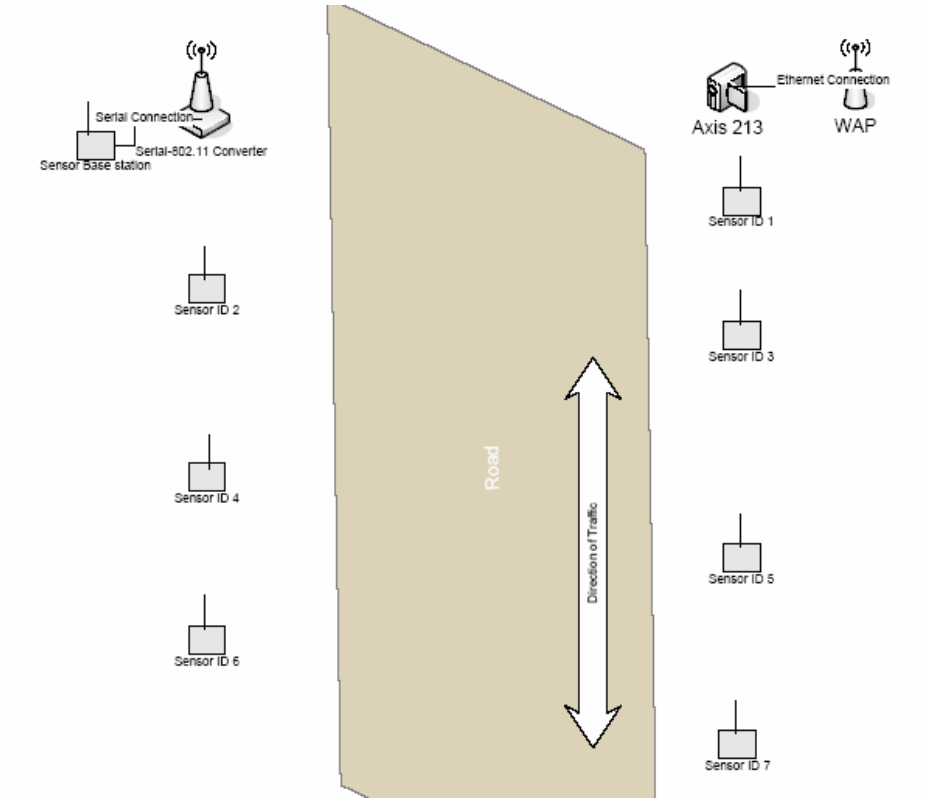

Figure 26. Deployment of Sensor Grid (COASTS OPORD, 2006).

C. EXPERIMENTAL DESCRIPTION AND RESULTS

The experiments conducted for this research involved the use of the Crossbow MSP410CA Mote Security System which contained 8 MSP410CA motes and 1 MBR410CA base station mote. A portable laptop was also required for the experiments. The user was required to install the Mote-View Client software into the laptop to acquire graphical interface with the deployed sensor nodes. Most of the experiments were conducted on the grounds of the Naval Postgraduate School in Monterey, California.

1. Indoor Radio Range Test

The first experiment conducted with the Crossbow sensor motes was the radio range test in an indoor environment. There are several factors that affect the

communication range of the MSP410CA motes: transmission power, antenna length, node elevation, and the effects of multi-path. Throughout the testing, the transmission power, antenna length, and node elevation were held constant. Transmission power and antenna length were set to maximum. The node elevation was leveled with the surface ground. Multi-path became relevant only when multiple motes were deployed.

The indoor testing was done inside a building with a hallway that extended 250 meters. The base station node was placed at the end of the hallway. One MSP410CA sensor mote was placed in front of the base station to establish connection. Afterward, the sensor mote was moved away from the base station until link connection was lost. The maximum range from mote to base station was determined to be 55 meters. When a second sensor mote was added to the test, it was determined that the maximum range from the sensor mote to the first mote was around 15 meters. When all eight motes were added into the network, nodes employed multi-paths with their nearest neighbors to reach the base station. The maximum perimeter of the senor network was over 152 meters.

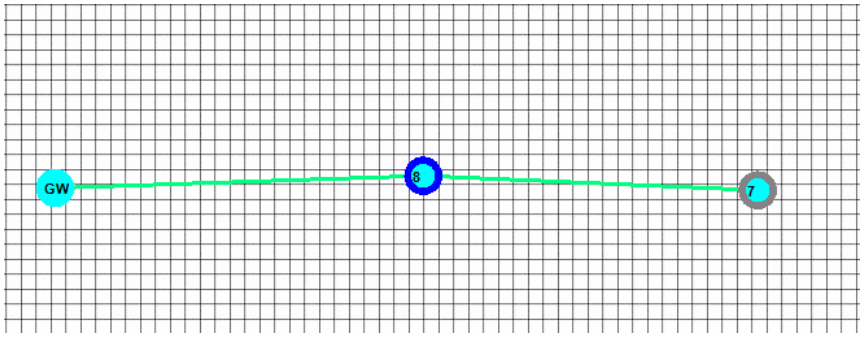

Figure 27. Topology View of Two Nodes and Base Station

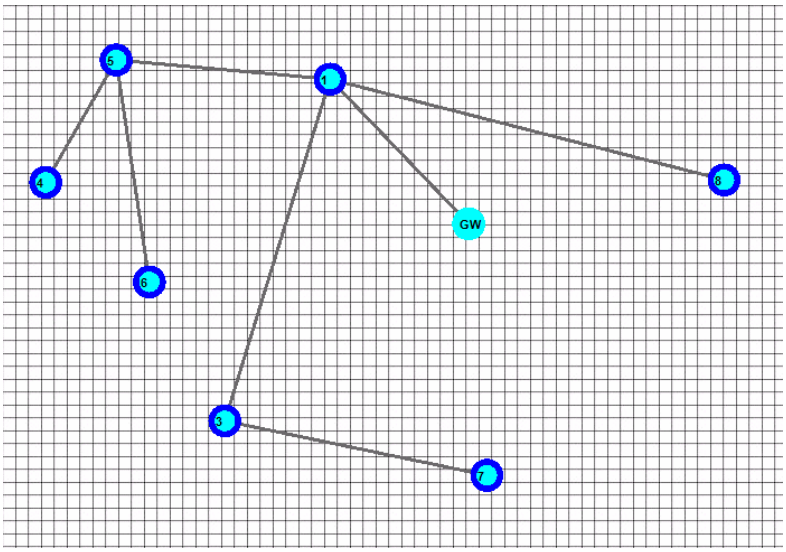

Figure 28. Nodes Employing Multi-path to reach Base Station

2. Grassy Outdoor Radio Range Test

The radio range test was repeated outdoor on a flat grassy surface. The maximum communication range that a sensor mote was able to connect with the base station was around 45 meters. The furthest distance apart that the sensor nodes could communicate with each other was 14 meters. During the experiment, detection ranges from the sensor motes were observed. Detection ranges were dependent on the type of object and its sizes. For a full size truck, the detection range was 50 meters. A medium size truck had a range of 40 meters, a car had a 35 meters range, and a person had a 10 meters range.

3. Wooded Outdoor Radio Range test

The last radio range test was conducted in a wooded environment that was not densely populated with trees. Communications among the sensors were established in this area. The maximum range observed from a single node to the base station was around 24 meters. Afterward, the other seven sensor motes were turned on and the maximum

separation distance among the motes was determined to be 9 meters. During the test, detection range was observed at 7 meters for people. When the range test was moved to a more densely wooded area, communication range dropped. The maximum range from base station to a single node was 12 meters and 4 meters for the sensor motes.

4. Battery Life Test

The last round of experiments focused on the battery life of the sensor motes. As mentioned previously, the MSP410 motes are powered by two AA batteries. The information obtained from Crossbow stated that the battery powered MSP410CA motes should last 96 hours. Table 6 below summarizes the MSP410CA power requirements for various operations.

Circuit	Mode	Current
PIR	Off	1 µA
PIR	On	300 µA
Magnetometer, per axis	Off	1 µA
Magnetometer, per axis	On	3 mA
Radio	Off	1 µA
Radio	RX mode	8 mA
Radio at 1 mW	TX mode	16 mA
Processor	Sleep	15 to 20 µA
Processor	Active	8 mA
Serial flash memory	Write	15 mA
Serial flash memory	Read	4 mA
Serial flash memory	Off	2 µA

Table 6. Power Requirements for MSP410CA Mote (Xbow.com, 2006).

The purpose of this experiment was to determine the levels of battery life for the motes by varying the distances of the motes to the base station. The experiment was done indoor employing one base station and five MSP410CA motes. The transmission power for all five motes was set to minimum and the antenna length was held constant at the maximum. In order to set the transmission power for the five motes, the user logged onto the Mote-View Client software and changed the parameter wirelessly. This was accomplished by clicking on the Command Tab. From the Command Window, the user selected the motes to alter and clicked on Radio Power to change the transmission power of the motes. The experiment could only be done indoor due to the power constraint of the MBR410CA base station and portable laptop. Both equipments required continuous power that is supplied by an AC power source. The five motes were powered by 2 Energizer Alkaline batteries that were rated at 1.50 volts and 2850 milliamp-hours for each cell. The batteries were recently bought and came from the same package.

MSP410CA Mote	Range to BS (meters)	Battery Life (hrs)
1	1.5	95.42
2	3	125.67
3	4.5	146.85
4	6	95.50
5	9	135.87

Table 7. Motes Battery Life.

Table 7 above provides an overview of the battery life test. The motes were deployed at various ranges from the base station. Two of the motes were operational for 95 hours. This figure was similar to the information Crossbow provided. The other three motes continued to operate long after the expected expiration time. The long battery life of these motes could be due to the short ranges to the base station. Also, the experiment was done in an indoor environment with ideal condition. Lastly, transmission power was set at the minimum level for the sensor motes. The experiment was inconclusive at determining the effect of deployment ranges on battery life. However, it did indicate that the motes could run continuous for over 95 hours.

D. DISCUSSION

WSNs are intended to be deployed for a long period of time with little or no user's involvement. This means that the battery life becomes a significant factor as it determines the operational time of the WSN. Therefore, the user must understand the requirements for selecting a battery. There are two types of battery. One type is primary which is for single use and the other type is secondary which is rechargeable. A primary battery is good for long term use or very low drain rates. A secondary battery is good for applications where access to power recharging is available. Another battery issue is the drain rate. The drain rate is dependent on the current usage of a device. It has been tested that alkaline battery is good under a wide range of loads, lithium coin cells are good under low loads, and lead-acid and NiCd cells are good at high rate applications (xbow.com, 2006). Temperature is another issue that the user must be aware of

when it comes to battery. Batteries don't charge or discharge well at low temperatures. Most batteries perform best in the -20°C to +60° range. Lithium battery does better than other batteries at both temperature extremes.

The selection of batteries is a deployment issue that a user must address. In the experiments with the MSP410CA motes, it is determined that the motes can operate for around 96 hours. However, the limited factor with the MSP410CA security system is the base station which requires continuous power. With this system, remote sensing is not feasible. The system works best in an industrial environment where power can be supplied to the base station.

Another issue that was brought up in the research experiments was the separation ranges among the MSP410CA motes and the base station. Prior to the user deploying the motes, he must be aware of the topology of his environment. The experiments showed that in a flat terrain environment, the ranges of the motes were much longer than the ranges of the motes that were deployed in a wooded environment. The deployment strategy would be different for an open area versus a dense environment. The spacing between motes must be examined as well as the number of motes to deploy to cover a desired area of interest. A wooded area would require shorter distance among the motes and more motes to cover a specific area.

Besides the various terrains that the user must consider prior to deployment, the weather and temperature must also be considered. The Crossbow user's manual stated that the MSP410CA motes could operate in a temperature range of 0 to 70°C. Unfortunately, the experiments did not

focus on the ranges of the temperature. As stated before, the experiments were completed on the grounds at NPS. During the various experiments, the temperatures ranged from 10°C to 20°C. The observed temperatures didn't affect the communication range or the detection range of the MSP410CA motes. The experiments were also limited by the lack of rain to determine how the rain would affect the ranges of the motes. In addition, the motes were never tested in severe weather conditions. In order for a user to deploy the sensor motes, he must take into account the weather, temperature, battery life, and the topology of the environment.

E. SUMMARY

This chapter explores the implementations and testing of Crossbow MSP410CA Mote Security System. It begins with the demonstration of the system by the COASTS project. Afterward, the security system is tested on the grounds of NPS. Experiments on the Crossbow security system to test the radio ranges and battery life of the sensor motes. These tests helped to determine the operational characteristics of the motes. Once these characteristics are explored and documented, the wireless sensors can be comfortably deployed to meet the needs of the operators. Given time, wireless technologies will be a common aspect of our daily lives.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

A. SUMMARY AND CONCLUSIONS

The continual improvement in technologies has enabled wireless sensors to be smaller and more capable. This has lead to the use of WSNs in many different areas of application. This thesis explores the field of WSNs and researches their military applications.

The thesis begins with an introduction to WSN in Chapter II. The characteristics, applications, and challenges of WSN are discussed. In addition, the history of the ZigBee Alliance is explained along with the development of the IEEE 802.15.4 study group. Chapter II also discusses the Physical Layer and MAC Layer in the 802.15.4 standard and the network topologies. Chapter III provides a discussion on the military applications of WSNs. It lists the objectives and criteria the military wants to achieve when it implements WSNs. Lastly, examples of military applications are discussed. Chapter IV describes the hardware and software technology offered by Crossbow. In particular, the chapter focuses on the MSP410CA Mote Security System. Chapter V begins with a discussion of the COASTS project and its implementation of the Crossbow MSP410CA security system. The second half of the chapter deals with the implementation and testing of the MSP410CA Mote Security System at NPS. The results from the tests are included in the chapter.

The study in wireless sensor networks is an ongoing process. This research deals with a small aspect of WSNs and it hopes to bring greater understanding in the deployment issues of WSNs and their military applications.

This research shows that WSN is a promising new technology that can be of great use to both the military and civilian sectors in dealing with monitoring and surveillance operations.

The experiments conducted with the Crossbow MSP410CA security system showed some strengths and weaknesses of the WSN. One of the strengths of the Crossbow surveillance system was its ease of use. The Crossbow motes and base station required little technical skill to operate. In addition, the Mote-View client software was intuitive and user friendly. Another strength of the surveillance system was its self-healing attribute. During the experiments, some of the motes would fall out of the network due to low batteries or being out of range. When this happened, other motes would reconnect with neighboring motes to maintain the network. In addition to the strengths, the Crossbow surveillance system also demonstrated some weaknesses. A crucial weakness of the system is the power requirement of the base station. The base station was not battery operated and it required continuous power. When experiments were conducted outdoor, the base station used power from the laptop. This power requirement limited the operation of the surveillance system to only an hour when it was used outdoor. When experiments were conducted indoor or around a perimeter of a building, another weakness was observed. In this environment, the base station was not limited by its need for power. However, the motes were limited to around 96 hours of battery life. Even though the surveillance system had some weaknesses, its strengths would enable many useful applications of monitoring.

The Crossbow surveillance system is an excellent example of how a WSN can be applicable for military use. The COASTS project indicates that the Crossbow surveillance system in combination with other WSN technology can promulgate real time information from the infantry level to the commander level. If the military is serious about the applications of a WSN similar to the Crossbow system, the military must keep in mind issues like interoperability and security. Can the military expect Crossbow equipments to interoperate with other vendors? Can the military be guaranteed that its WSNs are secured from enemy's spoofing? These questions are relevant to the development and applications of WSN. However, they have to be answered in later research.

B. RECOMMENDATIONS FOR FUTURE WORK

WSNs is a rapidly emerging area of technology. There are many researches being conducted on the various characteristics and applications of WSNs. This thesis experiments on the ranges and battery life of the Crossbow MSP410CA sensors. From the findings obtained from the experiments, a greater understanding of the deployment issues is achieved.

In order for WSNs to be applicable for the military, for remote surveillance applications, extending the battery life is an important issue. Even though wireless sensors are low cost, their longer operational time will make the deployment more attractive. The goal is to develop sensors that the military can deploy and leave them in an unattended mode for a long period of time. The sensors operate on their own for an extended time without fear of losing power. One solution to the power issue is to

incorporate renewable power for the sensors. By installing a solar cell on a sensor, it is feasible that the operational time of the sensor can be extended in sunny environment.

Another issue that the military must confront is the security aspect of WSNs. Prior to the implementation of a WSN in a military environment, security of the network and its equipments has to be enforced. Though the topic of security is not mentioned in this thesis, its relevance can not be understated. The applications of WSNs by the military imply that sensitive information is transmitted between nodes and base station. Security actions must be investigated to protect the WSNs from being penetrated by unauthorized enemy forces.

Security of the WSNs involves three aspects (confidentiality, authentication, and integrity). The confidentiality requirement is important to ensure that sensitive information is protected and not revealed to enemy forces. In a wireless sensor environment, confidentiality is needed to safeguard data that are transmitted between the nodes of the network. If confidentiality is lost, the enemy can use the stolen information to inflict damages to our military forces. Future work can discuss on ways the military can prevent adversaries from eavesdropping into the networks and stealing critical information.

Another security issue is the topic of authentication. Authentication is a technique that verifies the identity of the participants in the network. In a sensor networks environment, it is important that the sensor nodes and the base station can verify that the received data are actually

sent by a legitimate node. If the enemy is able to overcome the authentication protocol of the network, then false data are accepted as legitimate. False data can easily bring down the usefulness of the network and create great harms to our military forces. Additional research must be studied to ensure that the enemy can not inject a malicious node into a friendly force network to create false information.

The third aspect of security is integrity. Integrity deals with the legitimacy of the data when they are traveling over the wireless networks. The military must find ways to ensure that integrity is safeguarded so that the data are not intercepted and modified by the enemy. Data that are altered can be disastrous for the military. Unfortunately, if the military depends on WSN products that are bought commercially off-the-shelf, then there is a greater risk that the enemy has access to the similar products. With similar wireless sensors, the enemy is better equipped to breaching the security of the military network. Security issues like integrity, authentication, and confidentiality are important to the field of WSNs. In order for WSNs to be applicable to the military, more research into security must be explored. Though WSN is still a new technology, future research will enable secured and feasible applications for the military.

Technology has made tremendous advancement in the field of wireless communications. This thesis and future studies will open new possibilities and innovations that will make WSNs more accessible and feasible.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Baker, N. (2005, April/May). *Bluetooth: Strengths and Weaknesses for Industrial applications*. IEEE Computing & Control Engineering, 21-25.

Brownfield, M. (2005). *Wireless Sensor Network Denial of Sleep Attack.* Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 356-364.

Buschmann, C., Fekete, S., Pfisterer, D., Fischer, S., & Kroller, A. (2005). *Spyglass: A Wireless Sensor Network Visualizer.* ACM SIGBED Review, 2.

CC1000 Technical Information Data Sheet. www.chipcon.com/files/cc1000_data_sheet_2_2.pdf. Last accessed March 2006.

COASTS Operations Order (2006, March). *Operations Order 030-06 (Thailand Rehearsal)*. Naval Postgraduate School, Monterey, CA.

Craig, W.C. (2005). *ZigBee: Wireless Control that Simply Works*. ZigBee Alliance, Information and Resources, http://www.zigbee.org. Last accessed February 2006.

Ding, G., Bhargava, B., Sahinoglu, Z., & Zhang, P. (2005). *Reliable broadcast in ZigBee networks*. IEEE SECON Proceedings, 510-520.

Egan, D. ((2005, April/May). *The Emergence of ZigBee in Building Automation and Industrial Controls*. IEEE Computing & Control Engineering, 14-19.

Eicke, J. (2002, March). *Networked Sensors for the Objective Force*. U.S. Army Research Laboratory.

Everything You Always Wanted To Know About Sensor/Actuator Networks but Were Afraid to Ask. http://icapeople.epfl.ch/aad/teaching. Last accessed January 2006.

Geer, D. (2005, December). *Users Make a Beeline for ZigBee sensor Technology.* Computer, 16-19.

Hill, J., Horton, M., Kling, R., & Krishnamurthy, L. (2004, June). *The Platforms Enabling Wireless Sensor Networks.* Communications of the ACM, 47, 41-46.

Icus, K. (2006). *Beginner's Guide to Crossbow Motes.* Motes tutorials from http://www.pages.drexel.edu. Last accessed February 2006.

Kinney, P. (2003, October). *ZigBee Technology: Wireless Control that Simply Works.* Communications Design Conference from http://www.zigbee.org. Last accessed February 2006.

Koubaa, A., Alves, M., & Tovar, E. (2005, July). *IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview.* Technical Report from http://www.hurray.isep.ipp.pt. Last accessed on January 2006

Le, K. (2005, November). *ZigBee SoCs provide cost-effective solution*. Information and Resources from http://www.zigbee.org. Last accessed February 2006.

MSP410CA Mote Security System. www.xbow.com/Products/Products_pdf_files/Wireless_pdf. Last accessed February 2006.

Rajaravivarma, V., Yang, Y., & Yang, T. (2003, March). An *Overview of Wireless Sensor Network and Applications*. Proceedings of the 35th Southeastern Symposium, 432-436.

Scott, K. (2004, November). *Design and performance of IEEE 802.15.4. compliant MMSE Receivers*. Asilomar Conference on Signals, Systems and Computers, 2, 2051-2055.

Streeton, M. & Stanfield, C. (2005). *ZigBee: The telemetry solution?* IEEE RF & Microwave Engineering Professional Network, 8, 1-4.

Tingle, M. (2005, March). *Performance Evaluation of a Prototyped Wireless Ground Sensor Network*. Naval Postgraduate School, Monterey, CA.

Wadaa, A., Olariu, S., & Wilson, L. (2005). *Training wireless sensor network*. Mobile Networks and Application, 10, 151-168.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Prof. Gurminder Singh
   Naval Postgraduate School
   Monterey, California

4. Prof. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

5. LT Damian Ngo
   Naval Postgraduate School
   Monterey, California

6. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California